(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001 年9 月27 日 (27.09.2001)

PCT

(10) 国際公開番号
WO 01/71516 A1

(51) 国際特許分類[7]: G06F 15/00, 17/60

(21) 国際出願番号: PCT/JP01/02329

(22) 国際出願日: 2001 年3 月23 日 (23.03.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-128648 2000 年3 月23 日 (23.03.2000) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社タイテック (TIETECH CO., LTD.) [JP/JP]; 〒457-0071 愛知県名古屋市南区千竈通2丁目13番地1 Aichi (JP).

(71) 出願人 および
(72) 発明者: 橋本秀紀 (HASHIMOTO, Hideki) [JP/JP]; 〒107-0052 東京都港区赤坂9丁目5番27号 ルピナス赤坂乃木坂302号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 深津博一 (FUKATSU, Hirokazu) [JP/JP]; 〒457-0071 愛知県名古屋市南区千竈通2丁目13番地1 株式会社 タイテック内 Aichi (JP).

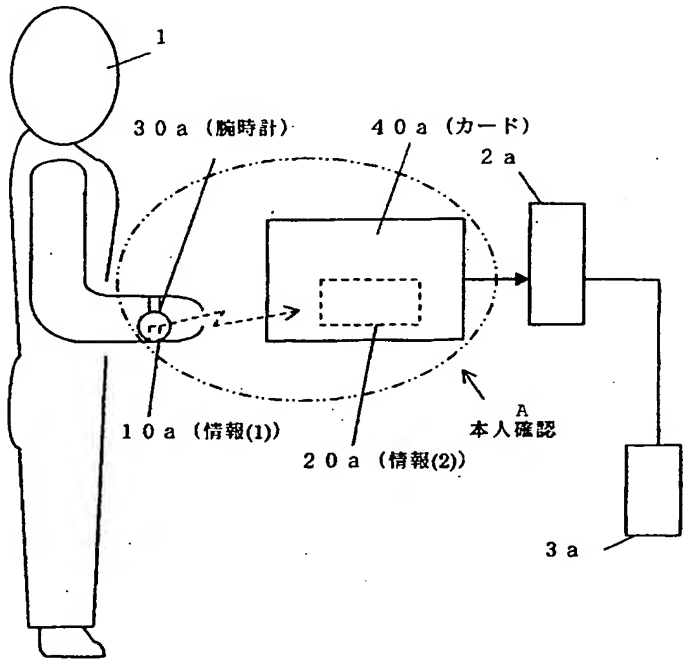
(74) 代理人: 岡田英彦, 外(OKADA, Hidehiko et al.); 〒460-0008 愛知県名古屋市中区栄二丁目10番19号 名古屋商工会議所ビル Aichi (JP).

(81) 指定国 (国内): US.

[続葉有]

(54) Title: METHOD AND APPARATUS FOR PERSONAL IDENTIFICATION

(54) 発明の名称: 本人確認方法及び本人確認装置



10a...(INFORMATION 1)
20a...(INFORMATION 2)
30a...(WRIST WATCH)
40a...(CARD)
A...PERSONAL IDENTIFICATION

(57) Abstract: A portable user unit (10a) is provided in a portable user device (30a) (such as a wrist watch or glasses), and a user unit (20a) is provided in a user device (40a) (such as a card or portable telephone). Original information is divided to form first information (1) and second information (2). The portable user unit (10a) stores the first information (1), and the user unit (20a) stores the second information (2) and the original information. The portable user unit (10a) transmits the first information (1) stored in itself. The user unit (20a) combines the received information (1) and the second information (2) stored by itself to form third information. If the third information agrees with the original information, the user is authenticated. Upon the authentication, the user device (20a) permits the user to use the user device (40a).

[続葉有]

WO 01/71516 A1

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

(57) 要約:

ユーザが携帯可能なユーザ携帯機器（腕時計、眼鏡等）３０ａに設けられるユーザ携帯装置１０ａと、ユーザが使用するユーザ機器（カードや携帯電話機）４０ａに設けられるユーザ装置２０ａを用いる。原情報を分割して第１情報(1)と第２情報(2)を形成する。第１情報(1)をユーザ携帯装置１０ａに記憶させ、第２情報(2)と原情報をユーザ装置２０ａに記憶させる。ユーザ携帯装置１０ａは、自身が記憶している第１情報(1)を送信する。ユーザ装置２０ａは、受信した情報(1)と自身が記憶している第２情報(2)を結合して第３情報を形成する。第３情報が原情報と一致する場合に、本人であると確認する。ユーザ装置２０ａは、本人であることを確認すると、ユーザ機器４０ａの使用を許可する。

明　　細　　書

本人確認方法及び本人確認装置

[技術分野]

本発明は、ユーザ機器を使用するユーザがそのユーザ機器の本来のユーザであることを（本人であること）を確認する本人確認方法及び本人確認装置に関する。特に、認証が必要であるシステムに好適に用いることができる本人確認方法及び本人確認装置に関する。さらには、本人確認装置の生成方法及び生成装置に関する。

[背景技術]

ユーザがサービス会社のサービスを利用する場合、サービス会社は、サービスを利用しようとするユーザが本人であることを確認するために、認証を行っている。

認証方法としては、例えば、暗証番号を用いる方法、サイン用いる方法、印章を用いる方法、ＩＤコードを用いる方法が使用されている。

暗証番号を用いる方法は、例えば、キャッシュカードを用いて銀行の口座から現金を引き出す場合に用いられる。ユーザは、現金を引き出す場合、銀行のＡＴＭ（現金自動支払機）のカード挿入口にキャッシュカードを挿入し、暗証番号を入力する。ＡＴＭは、キャッシュカードから読み取ったカード情報（例えば、ＩＤ）とユーザが入力した暗証番号を認証センタに送信する。認証センタは、ＡＴＭに入力された暗証番号及び読み取ったカード情報と、記憶手段に記憶されているカード情報と暗証番号との対応関係を含むデータベースに基づいて、認証を行う。

サインを用いる方法は、例えば、クレジットカードを用いて商品の代金を支払う場合に用いられる。ユーザは、クレジットカードで代金を支払う場合、商品購入票にサインをする。商品販売者は、商品購入票のサインとクレジットカードに記入されているサインを比較することによって認証を行う。

印章を用いる方法は、例えば、預金通帳を用いて銀行の口座から現金を引き出す場合に用いられる。ユーザは、預金通帳を用いて銀行の口座から現金を引き出す場合、現金引出用紙に印鑑を用いて押印する。銀行は、現金引出用紙に押印された印章と予め登録されている印章とを比較することによって認証を行う。

ＩＤコードを用いる方法は、例えば、ユーザが使用するユーザ機器の不正使用を防止する場合等に用いられる。この方法では、ユーザが携帯するタグ（例えば、送受信機能付きのカード）及びユーザが使用するユーザ機器（例えば、携帯電話機）に同じＩＤコードを記憶させる。タグは、ユーザ機器に接続して使用することもできるが、無線タグとして使用する場合が多い。ユーザ機器は、タグから送信されたＩＤコードと自己が記憶しているＩＤコードとを照合し、一致している場合にはユーザ機器の使用制限を解除（例えば、使用許可信号を出力）する。

また、他の認証方法として、各人に固有の生体情報（声紋、指紋、掌紋、網膜パターン、顔を撮像した画像等）を用いる方法が知られている。この認証方法では、生体情報読取装置によってユーザの生体情報を読み取り、読み取った生体情報と予め登録されている生体情報とを照合することによって認証を行うものである。この認証方法は、各人に固有の生体情報を用いるため、認証精度が高い。

暗証番号、サイン、印章やＩＤコードによって本人確認を行う従来の本人確認方法は、キャッシュカードを使用した人、クレジットカードを使用した人、預金通帳を使用した人、ＩＤコードを記憶したタグを携帯する人が本来のユーザでない場合でも、正しいユーザであると認証してしまうことがある。例えば、ユーザ機器（例えば、キャッシュカード）や印鑑等の盗難、暗証番号、サインやＩＤコード等の情報盗難や情報漏洩が発生すると、ユーザ機器が不正使用されてしまう。

また、生体情報によって本人確認を行う従来の本人確認方法は、生体情報読取装置（例えば、撮像装置）や生体情報処理装置（例えば、画像処理装置、大容量の記憶装置）等が必要であるため、システム全体のコストが高くなる。また、指に傷がついた場合や眼病になった場合には、指紋や網膜パターンが変化し、認証精度が低下する可能性がある。また、網膜パターンを用いる場合には、目を測定位置に持って行く必要があるため、煩わしさがある。また、指紋を用いる場合に

は、指を指紋読取装置に接触させる必要があるため、きれい好きの人にとっては心理的不快感がある。

[発明の開示]

本発明の目的は、低コストで信頼性の高い本人確認方法及び本人確認装置を提供することである。

本発明の本人確認方法及び本人確認装置は、一つの情報を複数の分割情報に分割し、一部の分割情報をユーザが携帯するユーザ携帯装置に記憶させ、他の分割情報をユーザが使用するユーザ機器に設けられるユーザ装置に記憶させる。ユーザ携帯装置は、自身が記憶している情報を送信する。ユーザ装置は、受信した情報と自身が記憶している情報とを結合し、所定の情報、例えば、原情報を復元できた場合に、そのユーザ機器の本来のユーザであることを確認し、ユーザ機器の使用を許可する。このように、本発明では、分割した情報を結合する処理だけでよいため、生体情報を用いる場合に比べて安価に構成することができる。また、例えば、カードやＩＤタグや暗証番号を盗まれても、ユーザ携帯装置及びユーザ装置を盗まれない限り、ユーザ機器が不正使用されることがない。このため、暗証番号、サイン、印章、ＩＤコード等を用いる場合に比べて信頼性が高い。

原情報としては記号、文字、図形、数式等種々の情報を用いることができる。また、原情報を分割する方法も、幾何学的に分割する方法、数式や論理式を用いて分割する方法等種々の方法を用いることができる。この点において、本発明の本人確認方法及び本人確認装置、汎用性がある。

使用するユーザ携帯装置の数は、２以上であってもよい。ユーザ携帯装置が２以上の場合には、使用するユーザ携帯装置の数とユーザ装置の数を加算した数だけ、原情報を分割する。使用する携帯装置の数が多いほど、信頼性は向上するが、結合処理は複雑になる。

本発明を用いた場合でも、ユーザ携帯装置とユーザ装置との間で送受信する情報が漏洩した場合には、ユーザ機器が不正使用される可能性がある。そこで、情報の漏洩を防止する対策を講じる必要がある。本発明の種々の実施例では、種々の情報漏洩防止技術が用いられている。

本発明の好ましい実施例では、送信側に暗号化装置を設け、受信側に復号化装置を設けている。これにより、送信側から受信側の情報を送信する際における、情報の漏洩を防止することができる。

本発明の他の好ましい実施例では、送信側に、原コードを所定の暗号化方法で暗号化した暗号化コードのみを記憶させ、受信側に、復号化方法と原コードを記憶させている。この場合、送信側には暗号化装置が設けられていないため、暗号化コードが漏洩しても、原コードを復号するのは困難である。

本発明の他の好ましい実施例では、暗号化方式として、時間的に変化する暗号化式を用いる暗号化方式を用いている。この実施例では、送信側装置には、任意の時点における暗号化式で原コードを暗号化した暗号化コードのみを記憶させ、受信側装置には、任意の時点における復号化式と原コードを記憶させる。時間的に変化する暗号化式としては、カオス演算式を用いるのが好ましい。カオス演算式を用いて暗号化された暗号化コードが漏洩しても、原コードを復号することはほとんど不可能であるため、信頼性が格段に向上する。

本発明の他の好ましい実施例では、暗号化方式として公開鍵暗号化方式を用いている。この実施例では、ユーザ装置は、ユーザ携帯装置から受信した第１の情報と自身が記憶している第２の情報を、公開鍵を用いて暗号化した暗号化コードを認証センタに送信する。認証センタは、公開鍵に対応する秘密鍵を用いて、受信した暗号化コードを復号化する。そして、第１の情報と第２の情報を結合して原情報を復元できるか否かを判断する。公開鍵暗号化方式を用いれば、公開鍵が漏洩しても暗号化コードを復号することができないため、信頼性が高い。また、１つの受信側に対して１つの公開鍵を割り当てればよいため、鍵の管理が容易である。公開鍵についても、原情報と同様に、例えば、第１公開鍵と第２公開鍵に分割してユーザ携帯装置とユーザ装置に記憶させれば、一層信頼線が高い。

本発明の他の好ましい実施例では、ユーザ機器に、ユーザ装置に記憶されている情報の不正な読み出しを検出した時に、情報の読み出しを禁止する読出禁止装置が設けられている。読出禁止装置としては、例えば、記憶装置を破壊する装置が用いられる。これにより、簡単な構成で、情報が不正に読み取られるのを防止することができる。

また、本発明の他の目的は、本人確認装置を容易に手に入れることができる本人確認装置の生成装置を提供することである。

本発明の好ましい実施例では、暗号装置と、原コード記憶装置と、暗号化コード記憶装置が設けられた回路基板を用意し、任意の時点で回路基板を切断することによって、送信側に設けられる第１の回路基板と、受信側に設けられる第２の回路基板を形成する。この方法を用いれば、暗号化機能を備えた本人確認装置を容易に得ることができる。

本発明の他の好ましい実施例では、ユーザが原情報を入力するとともに、分割方法を指示すると、入力された原情報が指示された分割方法で分割されて第１情報及び第２情報が形成され、第１情報が書き込まれたユーザ携帯装置及び第２情報が書き込まれたユーザ装置が商品排出口から排出される。これにより、ユーザは、容易に、自分の好みにあった本人確認装置を手に入れることができる。

本発明の目的及び利点は、以下に記載されている実施例の記載あるいはクレームを図面を参照しながら読むことによって、よりよく理解することができる。

[図面の簡単な説明]

図１は、本発明の本人確認方法の第１実施例を説明する図である。

図２は、本発明の本人確認方法における処理手順の例を説明する図である。

図３は、本発明の本人確認方法における処理手順の例を説明する図である。

図４は、分割情報を結合する例を説明する図である。

図５は、分割情報を結合する例を説明する図である。

図６は、本発明の本人確認装置の第１実施例のブロック図である。

図７は、ユーザ機器の１例を示す図である。

図８は、本発明の本人確認方法の第２実施例を説明する図である。

図９は、本発明の本人確認方法の第３実施例を説明する図である。

図１０は、本発明の本人確認方法の第４実施例を説明する図である。

図１１は、本発明の本人確認装置の第２実施例のブロック図である。

図１２は、本発明の本人確認装置の第３実施例のブロック図である。

図１３は、本発明の本人確認装置の第４実施例のブロック図である。

図１４は、本発明の本人確認装置の第５実施例のブロック図である。

図１５は、本発明の本人確認装置の第６実施例のブロック図である。

図１６は、本発明の本人確認装置の生成装置の一実施例のブロック図である。

図１７は、図１６に示す生成装置で生成したユーザ携帯装置及びユーザ装置の例を示す図である。

図１８は、本発明の本人確認方法の第４実施例を説明する図である。

図１９は、本発明の本人確認方法における処理手順の例を説明する図である。

図２０は、本発明の本人確認方法における処理手順の例を説明する図である。

図２１は、分割情報を結合する例を説明する図である。

図２２は、本発明の本人確認装置の第７実施例のブロック図である。

図２３は、本発明の本人確認装置の生成方法の一実施例を説明する図である。

図２４は、本発明の本人確認方法の第５実施例を説明する図である。

図２５は、本発明の本人確認装置の第８実施例のブロック図である。

図２６は、本発明の本人確認方法の第６実施例を説明する図である。

図２７は、本発明の本人確認方法の第７実施例を説明する図である。

図２８は、本発明の本人確認装置の第９実施例のブロック図である。

図２９は、分割情報を結合する例を説明する図である。

図３０は、分割情報を結合する例を説明する図である。

図３１は、本発明の本人確認装置の第１０実施例のブロック図である。

図３２は、本発明の本人確認装置の第１１実施例のブロック図である。

[発明を実施するための最良の形態]

以下に、本発明の好ましい実施例を図面を参照して説明する。

本発明に対応する本人確認方法の第１実施例を図１を用いて説明する。なお、図１は、本発明の本人確認方法を用いた認証システムを示している。

例えば、ユーザ１が、デビットカード（ユーザ機器）４０ａを用いて購入品の代金を支払う場合、従来の認証方法では、以下のようにしてユーザ認証が行われる。

まず、ユーザ１は、デビットカード４０ａを認証端末装置２ａのカード挿入口

に挿入するとともに、暗証番号を入力手段を用いて入力する。

認証端末装置２ａは、デビットカード４０ａに記憶されているカード情報（ＩＤ等）を読み取る。そして、読み取ったカード情報と、ユーザ１が入力した暗証番号を含むユーザ情報を認証センタ３ａに送信する。

認証センタ３ａの記憶装置には、暗証番号をカード情報と対応させたデータベースが記憶されている。認証センタ３ａは、認証端末装置２ａから送信されたユーザ情報に含まれているカード情報及び暗証番号とデータベースに記憶されている情報とを照合することによって認証を行う。

認証センタ３ａは、認証がＯＫであれば、認証ＯＫ信号を認証端末装置２ａに送信する。一方、認証がＮＧであれば、認証ＮＧ信号を認証端末装置２ａに送信する。

この認証処理では、前述したように、ユーザ１がデビットカード４０ａの本来のユーザであることの確認（本人確認）は行われていない。そこで、本実施例では、認証センタ３ａでユーザ認証処理が行われる前に、本人確認処理（図１の二点鎖線で囲んだ部分）が以下のように行われる。

本実施例の本人確認装置は、ユーザ１が携帯する腕時計（ユーザ携帯機器）３０ａに設けられたユーザ携帯装置１０ａと、ユーザが使用するデビットカード（ユーザ機器）４０ａに設けられたユーザ装置２０ａにより構成されている。ユーザ携帯装置１０ａとユーザ装置２０ａは、例えば、ユーザ認証を行うサービス会社が用意する。ユーザ携帯装置１０ａ、ユーザ装置２０ａを、ユーザ携帯機器３０ａ、ユーザ機器４０ａに取り付ける方法は種々の方法が可能である。例えば、接着剤や接着テープ等を用いて取り付ける方法、ユーザ携帯機器３０ａやユーザ機器４０ａに内蔵する方法等を用いることができる。

また、本実施例では、ユーザ装置２０ａは、本人であることを確認できるまでは、使用禁止信号を出力してデビットカード４０ａを使用不能状態とする。すなわち、認証端末装置２ａがデビットカード４０ａのカード情報を読み出すことができないようにする。

ユーザ携帯装置１０ａとユーザ装置２０ａには、本人確認に必要な情報が記憶されている。例えば、元々一つの情報として認識される情報（原情報）を２つに

分割し、第１の分割情報（情報(1)）を、ユーザ携帯機器３０ａに設けられたユーザ携帯装置（１０ａ）に保有（記憶）させ、第２の分割情報（情報(2)）を、ユーザ機器４０ａに設けられたユーザ装置２０ａに保有（記憶）させる。原情報を分割する方法としては、種々の方法を用いることができる。

ユーザ携帯機器３０ａは、腕時計に限定されず、ユーザ１が携帯可能あるいは携行可能であればよい。例えば、指輪、眼鏡、ベルトのバックル、ブレスレット、ペンダント、イアリング、ピアス、財布、定期券、免許証等を用いることができる。ユーザ携帯装置１０ａは、ユーザ携帯機器３０ａと共に携帯する必要はなく、例えば、ポケットやカバンに入れて携帯してもよい。ユーザ機器４０ａは、カードに限定されず、本人確認が必要な機器であればよい。例えば、携帯電話機やパソコン等でもよい。ユーザ機器４０ａは、複数のユーザが共用するものであってもよい。

ユーザ携帯装置１０ａは、第１の情報(1)をユーザ装置２０ａに送信する送信手段を備えている。第１の情報(1)を送信する方法としては、無線電波を用いてもよいし、超音波や光（赤外線）を用いてもよい。

ユーザ装置２０ａは、第１の情報(1)を受信すると、受信した第１の情報(1)と自身が記憶している第２の情報(2)を所定のアルゴリズム（結合方法）で結合して第３の情報(3)を作成（形成）する。そして、第３の情報(3)と原情報を照合することによって本人確認を行う。すなわち、受信した第１の情報(1)と自身が記憶している第２の情報(2)を結合して原情報を再生あるいは復元することができた場合に、本人であることを確認する。前記したように、対応するユーザ携帯装置１０ａとユーザ装置２０ａには、同一の原情報から生成された第１の情報(1)と第２の情報(2)を記憶させている。このため、ユーザ装置２０ａは、第２の情報(2)に対応する第１の情報(1)を受信した場合にだけ、原情報を再生あるいは復元することができる。

図１に示す認証システムでは、デビットカード（ユーザ機器）４０ａに記憶されているカード情報は、ユーザ装置２０ａがユーザ１が本人であることを確認した場合にのみ出力される。

例えば、紛失しあるいは盗まれたデビットカード４０ａを第三者が使用しよう

としても、ユーザ装置２０ａは、デビットカード４０ａの本来のユーザ１が携帯しているユーザ携帯装置１０ａから送信される第１の情報(1)を受信することができない。このため、認証センタ３ａでユーザ認証が行われる前に、デビットカード４０ａに設けられているユーザ装置２０ａの本人確認処理によって不正使用を確実に阻止することができる。

本実施例では、割り符のように、一つの原情報を第１の情報(1)と第２の情報(2)に分割し、第１の情報(1)をユーザ携帯装置１０ａに記憶させ、第２の情報(2)をユーザ装置２０ａに記憶させている。そして、ユーザ装置２０ａは、受信した情報と自身が記憶している情報とを結合して、原情報を形成することができた場合にのみ本人であることを確認する。したがって、生体情報を用いる場合に比して、安価に構成することができる。また、暗証番号やカードを盗まれたり、紛失したりしても、ユーザ携帯機器（ユーザ携帯装置）を盗まれたり、紛失したりしない限り、不正使用の心配がない。また、ユーザ携帯装置１０ａとユーザ装置２０ａには異なる情報を記憶させているので、一方が盗まれたり、紛失しても不正使用の心配がない。したがって、暗証番号、サイン、ＩＤデータ等を用いる場合に比べて、信頼性が高い。

なお、本実施例は、ユーザがユーザ機器を使用する際に、ユーザがそのユーザ機器の本当のユーザであるか否かを確認（本人確認）するための方法に関するものである。したがって、ユーザ機器で本人確認処理を行った結果をどのように利用するかは、ユーザ機器の種類やユーザ機器を利用する形態に応じて適宜選択される事項である。例えば、図１に示す実施例では、ユーザ装置２０ａは、本人であることを確認すると、デビットカード（ユーザ機器）４０ａのカード情報の認証端末装置２ａへの出力を許可する。これにより、デビットカード４０ａのカード情報が認証端末装置２ａで読み取られる。また、ユーザ１は、認証端末装置２ａの入力手段を用いて暗証番号を入力する。以後は、従来と同様の手順で、認証センタ３ａでユーザ認証処理（デビットカードの正当性を認証する処理）を行う。

図２は、本発明の本人確認方法における処理手順の例を説明する図である。本実施例では、ユーザ装置２０は、常時本人確認処理を行う。本実施例では、①～

④の手順で本人確認処理が行われる。

①ユーザ携帯装置１０は、適宜の時期に（例えば、所定の時間間隔で）、自身が記憶している第１の情報(1)を送信する。

②受信待機状態にあるユーザ情報２０は、情報(1)を受信する。

③ユーザ装置２０は、情報(1)を受信すると、受信した情報(1)と自身が記憶している第２の情報(2)を所定のアルゴリズムで結合して第３の情報(3)を形成する。

③ユーザ装置２０は、第３の情報(3)と原情報を照合して、第３の情報(3)と原情報が一致した場合に、ユーザが本人であることを確認する。すなわち、情報(1)と情報(2)を結合して原情報を形成することができた場合に、本人であることを確認する。

図３は、本発明の本人確認方法における処理手順の他の例を説明する図である。本実施例では、ユーザ装置は、本人確認が必要な場合に本人確認処理を行う。本実施例では、①～⑥の手順で本人確認処理が行われる。

①ユーザ装置２０は、本人確認処理を行う必要がある場合（例えば、デビットカードが認証端末装置のカード挿入口に挿入された場合等）に、第１の情報(1)の送信を要求する送信要求信号を送信する。

②受信待機状態にあるユーザ携帯装置１０は、送信要求信号を受信する。

③ユーザ携帯装置１０は、送信要求信号を受信すると、自身が記憶している第１の情報(1)を送信する。

④受信待機状態にあるユーザ装置２０は、情報(1)を受信する。

⑤ユーザ装置２０は、情報(1)を受信すると、受信した情報(1)と自身が記憶している第２の情報(2)を所定のアルゴリズムで結合して第３の情報(3)を形成する。

⑥ユーザ装置２０は、第３の情報(3)と原情報を照合し、第３の情報(3)が原情報と一致する場合に、本人であることを確認する。

なお、ユーザ装置２０は、情報(1)を受信できない場合、あるいは受信した情報(1)が正しい第１の情報(1)でない場合には、所定の処理を実行する。例えば、送信要求信号を送信した後、所定時間内に情報(1)を受信できない場合には、再度送信要求信号を送信する。そして、所定回数送信要求信号を送信しても情報(1)を受信できない場合には、本人を確認できないと判断し、所定の終了処理を実行

する。例えば、エラーメッセージを認証端末装置に表示させる。

次に、原情報を分割した分割情報を結合する方法を具体的に説明する。

図４に示す例は、原情報［０１１１］を第１の情報(1)［００１１］と第２の情報(2)［０１０１］に分割している。そして、第１の情報(1)をユーザ携帯装置１０に記憶させ、第２の情報(2)と原情報をユーザ装置２０に記憶させている。

ユーザ装置２０は、情報(1)を受信すると、受信した情報(1)と自身が記憶している第２の情報(2)を所定のアルゴリズムで結合して第３の情報(3)を形成する。本実施例では、受信した情報(1)と第２の情報(2)をＯＲ処理する。受信した情報(1)が正しい第１の情報(1)の場合には、受信した情報(1)と第２の情報(2)をＯＲ処理することによって、原情報［０１１１］が形成される。さらに、第３の情報(3)と原情報とを照合して本人確認を行う。本実施例では、第３の情報(3)が原情報と同じである否かを判断している。例えば、第３の情報(3)と原情報をＸＯＲ（排他的論理和）処理する。

分割方法は、図４に示した例に限定されず、分割した第１の情報(1)と第２の情報(2)を所定の論理演算することによって原情報を形成することができればよい。

図５に示す例では、原情報［数字７の図形のビット行列］を、図５に一点鎖線で示す、左右に引いた分割線を境に、上部の第１の情報(1)と下部の第２の情報(2)に分割している。そして、第１の情報(1)をユーザ携帯装置１０に記憶させ、第２の情報(2)と原情報をユーザ装置２０に記憶させている。

ユーザ装置２０は、情報(1)を受信すると、受信した情報(1)と自身が記憶している第２の情報(2)を所定のアルゴリズムで結合して第３の情報(3)を形成する。本実施例では、受信した情報のビット行列と情報(2)のビット行列を結合する。受信した情報(1)が正しい第１の情報(1)である場合には、受信した情報(1)のビット行列と第２の情報(2)のビット行列を結合すると、原情報［数字７の図形のビット行列］が形成される。さらに、第３の情報(3)と原情報を照合して本人確認を行う。本実施例では、第３の情報(3)のビット行列で表される図形が、原情報のビット行列で表される図形と同じであるか否かを判断する。

分割線を引く場所、引き方、分割線の本数等は、適宜選択可能である。また、

原情報を分割する数や分割する位置等は種々変更可能である。例えば、原情報を情報(a1)、情報(a2)、情報(a3)に分割し、情報(a1)と情報(a3)を第１の情報(1)とし、情報(a2)を第２の情報(2)としてもよい。

また、第１の情報(1)及び第２の情報(2)として同じ情報を用いることもできる。この場合、例えば、第２の情報(2)［０１１１］(＝第１の情報(1))と原情報［００００］をユーザ装置２０に記憶させる。ユーザ装置２０は、受信した情報(1)と自身が記憶している第２の情報(2)をＸＯＲ処理して第３の情報(3)を形成する。そして、第３の情報(3)と原情報を照合して本人確認を行う。

受信した情報と自身が保有している情報を結合するアルゴリズムは、原情報を分割する分割方法によって決定される。

次に、本発明の本人確認装置の第１実施例のブロック図を図６に示す。本実施例の本人確認装置は、ユーザ携帯装置１０ｂとユーザ装置２０ｂを有している。

ユーザ携帯装置１０ｂは、信号出力装置１１ｂ、変調／復調装置１２ｂ、通信装置１３ｂにより構成されている。信号出力装置１１ｂは、例えば、第１の情報(1)を記憶する記憶装置を有し、第１の情報(1)を出力する。第１の情報(1)の形式としては、種々の形式を用いることができる。

変調／復調装置１２ｂは、信号出力装置１１ｂから出力される第１の情報(1)を変調し、通信装置１３ｂを介してユーザ装置２０ｂに送信する。あるいは、変調／復調装置１２ｂは、通信装置１３ｂを介して受信した信号を復調する。そして、復調した信号に送信要求信号が含まれている場合には、第１の情報(1)を変調し、通信装置１３ｂを介して送信する。ユーザ携帯装置１０ｂには、各構成装置に電力を供給する電池が設けられている。

ユーザ装置２０ｂは、通信装置２１ｂ、変調／復調装置２２ｂ、結合装置２３ｂ、信号出力装置２４ｂを有している。変調／復調装置２２ｂは、通信装置２１ｂを介して受信した信号を復調し、結合装置２３ｂに出力する。あるいは、変調／復調装置２２ｂは、送信要求信号を変調し、通信装置２１ｂを介してユーザ携帯装置１０ｂに送信する。そして、その後に通信装置２１ｂを介して受信した信号を復調し、結合装置２３ｂに出力する。

信号出力装置２４ｂは、例えば、第２の情報(2)を記憶する記憶装置を有し、

第２の情報(2)を出力する。結合装置（本人確認装置）２３ｂは、変調／復調装置２２ｂから入力された情報(1)と第２の情報(2)を所定のアルゴリズムで結合して第３の情報(3)を形成する。例えば、割り符を合わせる方法を用いて第１の情報(1)と第２の情報(2)を結合する。さらに、結合装置２３ｂ（本人確認装置）は、第３の情報(3)と原情報の照合結果に基づいて本人か否かを確認する。結合装置２３ｂは、信号出力装置２４ｂあるいは変調／復調装置２２ｂと一体に設けてもよい。ユーザ装置２０ｂには、各構成装置に電力を供給する電池が設けられている。

結合装置２３ｂは、例えば、本人が確認されていない時に出力禁止信号を出力する。結合装置２３ｂから出力禁止信号が出力されている場合には、ユーザ機器は使用不能となる。例えば、デビットカードに記憶されているカード情報を認証端末装置で読み取ることができない、あるいは携帯電話を使用することができない。なお、原情報を信号出力装置２４ｂに記憶させてもよい。

ユーザ装置とユーザ機器が別体の場合には、ユーザ装置（結合措置）とユーザ機器との間の信号の伝送は、無線あるいはケーブルを介して行われる。ユーザ装置及びユーザ機器に互いに接続可能な接続端子を設けておけば、接続端子同士を接続するだけでユーザ装置とユーザ機器を接続することができるため、接続作業が容易となる。

ユーザ携帯装置１０ｂの信号出力装置１１ｂ、変調／復調装置１２ｂ、通信装置１３ｂや、ユーザ装置２０ｂの通信装置２１ｂ、変調／復調装置２２ｂ、結合装置２３ｂ、信号出力装置２４ｂは、ハードウェアで実現してもよいし、ソフトウェアで実現してもよい。

本実施例の結合装置２３ｂが、本発明の本人確認装置に対応する。

図７は、ユーザ機器４０ｂの１例の斜視図である。図７に示すユーザ機器４０ｂは、カード状に形成されている。カードの内部には、図６に示した各構成装置２１ｂ～２４ｂが設けられている。ユーザ機器４０ｂは、ユーザ携帯装置１０ｂと通信を行う通信機能を備えた通信機器でもある。ユーザ機器４０ｂとしては、磁気カード、ＩＣカード、デビットカード、クレディットカード、キャッシュカード等を用いることができる。例えば、デビットカード、クレディットカードま

たはキャッシュカード等の決済用カードに通信機能を持たせることによって、決済用カードに本人確認機能を持たせることができる。なお、カードは、決済用カードや金融用カードに限定されるものではなく、無線機等の通信機器をカード状に形成したものでもよいことは、勿論である。

図８は、本発明の本人確認方法の第２実施例を説明する図である。本実施例では、携帯電話機４０ｃをユーザ機器として用いている。本実施例では、ユーザ装置２０ｃは、本人確認処理を行い、その結果に基づいて携帯電話機４０ｃの使用を許可するか否かを判断する。例えば、携帯電話機４０ｃに設けられているユーザ装置２０ｃは、ユーザ携帯装置１０ｃから送信される情報(1)が、自身が記憶している第２の情報(2)に対応する正しい第１の情報(1)である場合にのみ、携帯電話機４０ｃの使用を許可する。これにより、携帯電話機４０ｃの不正使用を防止することができる。

ユーザ機器４０ｃとしては、携帯電話機の他に、通信機能を備える各種の機器を用いることができる。例えば、ＰＨＳ（Personal Handyphone System）電話機、ＰＤＡ（Personal Data Assistance、個人用携帯情報端末）無線機、ＥＴＣ（Electronic Toll Collection System, ノンストップ自動料金支払システム）用通信機、ＩＴＳ（Intelligent Transport Systems, 高度道路交通システム）用の車両通信機、電話通信端末（例、公衆電話機、ＦＡＸ端末)、データ通信端末（例、パソコン）等を用いることができる。何をユーザ機器として用いるかは、営業上または設計上の選択事項である。また、携帯電話機４０ｃと端末装置２ｃとの接続は、通信回路網４ｃを介して行ってもよい。携帯電話機４０ｃと端末装置（例えば、認証端末装置）２ｃとの間の接続方法や通信方法は種々の方法を用いることができる。

図９は、本発明の本人確認方法の第３実施例を説明する図である。本実施例では、ユーザ携帯装置１０ｄをＩＣチップで構成し、指輪（ユーザ携帯機器）３０ｄに取り付けている。勿論、ユーザ携帯装置１０ｄは、指輪以外のユーザ携帯機器に取り付けることができる。例えば、ベルトのバックル、ブレスレット、ペンダント、イアリング、ピアス等に取り付けることができる。本実施例では、ユーザ装置２０ｄもＩＣチップで構成し、無線機４０ｄに取り付けている。

ＩＣチップは、集積回路（ＩＣ）をパッケージあるいはモールドし、リード線（外部端子）を備えるＩＣ製品である。ＩＣには、ＬＳＩ(Large Scale Integration）やＶＬＳＩ等も当然に含まれる。回路の集積度は問題ではない。なお、ユーザ携帯装置及びユーザ装置のいずれかをＩＣチップとしてもよいし、両方をＩＣチップとしてもよいことは言うまでもない。さらに、ユーザ装置及びユーザ装置の一部をＩＣチップとしてもよい。

図１０は、本発明の本人確認方法の第４実施例を説明する図である。本実施例では、ユーザ携帯装置１０ｅを眼鏡（ユーザ携帯機器）３０ｅに、例えば接着剤を用いて取り付けている。また、携帯電話機４０ｅをユーザ機器として用いている。ユーザ携帯装置１０ｅとユーザ装置２０ｅとの間の通信は無線で行っている。ユーザ装置２０ｅの送信装置として携帯電話機４０ｅの通信装置を用いることもできる。

ユーザ携帯装置１０ｅは、ＩＣチップでもよい。携帯電話機４０ｅに代えて、ＩＣカードやＩＣカード製のデビットカード等を用いてもよい。あるいは、携帯電話機能付きのＩＣカード等を用いることもできる。また、ユーザ携帯装置１０ｅは、眼鏡以外のもの、例えば、ブレスレットやベルト等に取り付けてもよい。ユーザ携帯装置１０ｅを、ユーザ携帯機器に取り付けず、ユーザ１のポケットやカバンに入れて持ち歩いてもよい。

図１１は、本発明の本人確認装置の第２実施例のブロック図である。本実施例では、ユーザ携帯装置１０ｆやユーザ装置２０ｆの構成要素の一部あるいは全部をＩＣチップで構成している。図１１に示す実施例では、ユーザ携帯装置１０ｆの信号出力装置１１ｆ、変調／復調装置１２ｆ及び通信装置１３ｆのそれぞれをＩＣチップで構成している。もちろん、これら３つの手段を一つのＩＣチップで構成することもできる。

また、ユーザ装置２０ｆの信号出力装置２４ｆをＩＣチップで構成している。

なお、ユーザ装置２０ｆの通信装置２１ｆ、変調／復調装置２２ｆ、結合装置２３ｆ及び信号出力装置２４ｆを一つのＩＣチップ２５ｆで構成することもできる。

図１２は、本発明の本人確認装置の第３実施例のブロック図である。本実施例

では、ユーザ装置２０ｇに破壊装置２６ｇを設けている。破壊装置２６ｇは、例えば、信号出力装置２４ｇに記憶されている第２の情報(2)の不正な読み出しを検出した場合に、信号出力装置２４ｇから所定の情報が外部に出力されるのを阻止する。

不正な読み出しの検出は、例えば、通信装置２１ｇで受信した信号に、正規の読み出し信号以外の読み出し信号が含まれていることにより検出する。信号出力装置２４ｇからの信号出力を阻止する方法としては、例えば、信号出力装置２４ｇに過電流を流し、信号出力装置２４ｇを破壊する方法を用いることができる。あるいは、揮発性の記憶装置に情報等を記憶させている場合には、記憶装置への電源供給を遮断し、記憶装置に記憶されている情報等を消去する方法を用いてもよい。

破壊装置２６ｇは、ユーザ装置２０ｇが分解されることを検出した場合に、信号出力装置２４ｇあるいはユーザ装置２０ｇを破壊するものでもよい。

本実施例の破壊装置２６ｇが、本発明の読出禁止装置に対応する。

図１３は、本発明の本人確認装置の第４実施例のブロック図である。ユーザ携帯装置１０ｈは、信号出力装置１１ｈ、変調／復調装置１４ｈ、通信装置１３ｈにより構成されている。ユーザ装置２０ｈは、通信装置２１ｈ、変調／復調装置２７ｈ、結合装置２３ｈ、信号出力装置２４ｈにより構成されている。本実施例では、ユーザ携帯装置１０ｈの変調／復調装置１４ｈに、暗号化機能を持たせている（暗号化機能及び復号化機能を持たせる場合もある）。また、ユーザ装置２０ｈの変調／復調装置２７ｈに、復号化機能を持たせている（暗号化機能及復号化機能を持たせる場合もある）。

本実施例では、ユーザ携帯装置１０ｈは、第１の情報(1)を暗号化して送信する。そして、ユーザ装置２０ｈは、受信した信号の暗号を解読して情報(1)を得る。これにより、セキュリティが一層向上する。なお、ユーザ装置２０ｈからユーザ携帯装置１０ｈに信号を送信する時にも、信号を暗号化して送信することもできる。

暗号化処理と復号化処理を同じ装置で行ってもよいし、異なる装置で行ってもよい。暗号化方法としては、公知の種々の暗号化方法を用いることができる。

図１４は、本発明の本人確認装置の第５実施例のブロック図である。ユーザ携帯装置１０ｉは、信号出力装置１１ｉ、変調／復調装置１５ｉ、通信装置１３ｉにより構成されている。ユーザ装置２０ｉは、通信装置２１ｉ、変調／復調装置２８ｉ、結合装置２３ｉ、信号出力装置２４ｉにより構成されている。本実施例では、ユーザ携帯装置１０ｉの変調／復調装置１５ｉに、送信信号にランダムノイズ（ＲＮ）を挿入する機能を持たせている（ＲＮ挿入機能及びＲＮ除去機能を持たせる場合もある）。また、ユーザ装置２０ｉの変調／復調装置２８ｉに、受信した信号からランダムノイズ（ＲＮ）を除去する機能を持たせている（ＲＮ挿入機能及びＲＮ除去機能持たせる場合もある）。本実施例では、ユーザ携帯装置１０ｉは、第１の情報(1)にランダムノイズを挿入して送信する。これにより、セキュリティが一層向上する。

ランダムノイズ挿入処理とランダムノイズ除去処理を同じ装置で行ってもよいし、異なる装置で行ってもよい。信号の漏洩を防止する手段としては，ランダムノイズを挿入する方法以外にも公知の種々の方法を用いることができる。

図１５は、本発明の本人確認装置の第６実施例のブロック図である。ユーザ携帯装置１０ｊは、信号出力装置１１ｊ、変調／復調装置１２ｊ、通信装置１３ｊにより構成されている。ユーザ装置２０ｊは、通信装置２１ｊ、変調／復調装置２２ｊ、結合装置２３ｊ、信号出力装置２４ｊ、破壊装置２６ｊにより構成されている。

暗号化機能やＲＮノイズ挿入機能を用いても、本人確認情報である第１の情報(1)や第２の情報(2)が第三者に漏れる可能性はある。

第１の情報(1)あるいは第２の情報(2)が漏れている可能性がある場合には、第１の情報(1)及び第２の情報(2)を交換すればよい。そこで、本実施例では、ユーザ携帯装置１０ｊの信号出力装置１１ｊ、ユーザ装置２０ｊの信号出力装置２４ｊを交換可能に構成している。例えば、ユーザ携帯装置１０ｊの信号出力装置１１ｊ、変調／復調装置１２ｊ及び通信装置１３ｊを一つのＩＣチップ１６ｊで構成している。また、ユーザ装置２０ｊの通信装置２１ｊ、変調／復調装置２２ｊ、結合装置２３ｊ、信号出力装置２４ｊ及び破壊装置２６ｊを一つのＩＣチップ２５ｊで構成している。そして、必要な場合には、ユーザ携帯装置１０ｊのＩＣ

チップ１６ｊを交換用のＩＣチップ１７ｊに、また、ユーザ装置２０ｊのＩＣチップ２５ｊを交換用のＩＣチップ２７ｊに交換する。

なお、ＩＣチップの構成は種々変更可能である。例えば、ユーザ携帯装置１０ｊの信号出力装置１１ｊ、ユーザ装置２０ｊの信号出力装置２４ｊのみを交換可能に構成することもできる。また、ＩＣチップを交換可能に構成する方法としては、例えば、ピンやソケットにＩＣチップを差し込む構造にする方法等がある。

次に、本発明の本人確認装置を生成する生成装置の一実施例を図１６に示す。

本実施例の生成装置は、管理装置５０、端末装置６１～６３により構成されている。管理装置７０と各端末装置６１～６３は、通信回線（例えば、インターネット、電話回線等）７０により接続されている。通信回線としては、無線回線を用いることもできる。端末装置６１～６３は、例えば、コンビニや金融機関等に設置することができる。管理装置５０の設置場所は限定されず、また、端末装置６１～６３が兼用してもよい。

管理装置５０は、各端末装置６１～６３で本人確認装置を生成する際に端末装置６１～６３の表示手段６１ｂに表示する表示画面の画面情報、入力された原情報を指示された分割方法で分割するプログラム等が記憶された記憶装置を有している。

各端末装置６１～６３には、ＣＰＵ等の処理装置６１ａ、表示装置６１ｂ、入力装置６１ｃ、情報書込装置６１ｄ、商品排出装置６１ｅ等が設けられている。

入力装置６１ｃとしては、入力キー、記憶媒体に記憶されている情報を読み取る情報読取装置、画像情報を読み取る画像情報読取装置、表示装置の画面を指や入力ペンでタッチするタッチ式入力装置等を用いることができる。

情報書込装置６１ｄは、本人確認装置を構成するユーザ携帯装置の記憶装置及びユーザ装置の記憶装置に情報（第１の情報(1)、第２の情報(2)）を書き込むことができれば接触式、非接触式の種々の情報書込装置を用いることができる。接触式の情報書込装置を用いる場合には、ユーザ携帯装置やユーザ装置の端子を情報書込装置の端子に位置決めする位置決め手段を設けるのが好ましい。

商品排出装置６１ｅは、情報書込装置６１ｄによって情報が書き込まれたユーザ携帯装置及びユーザ装置を商品排出口、例えば、コンビニに設置されている端

末装置に設けられた商品排出口から排出する。

次に、本実施例の生成装置を用いて本人確認装置を生成する処理を説明する。なお、以下では、端末装置６１がコンビニに設置され、ユーザが端末装置６１を用いて本人確認装置を購入する場合について説明する。

また、端末装置６１内に、ユーザ携帯装置及びユーザ装置が、情報書込装置６１ｄにより情報が書込み可能に収納されているものとして説明する。

本人確認装置を購入するユーザは、まず、端末装置６１の表示装置６１ｂに表示されているメニュー画面で「本人確認装置の販売」を選択する。端末装置６１ｂの処理装置６１ａは、メニュー画面で「本人確認装置の販売」が選択されると、管理装置５０に「本人確認装置購入」信号を送信する。

管理装置５０は、端末装置６１から「本人確認装置購入」信号を受信すると、端末装置６１の表示装置６１ｂに原情報入力表示画面を表示させるための入力画面情報を端末装置６１に送信する。これにより、端末装置６１の処理装置６１ａは、原情報入力画面を表示装置６１ｂに表示する。

ユーザは、表示装置６１ｂに原情報入力画面が表示されている状態で、まず、入力装置６１ｃを用いて原情報を入力する。原情報を入力する方法としては、種々の方法を用いることが可能である。例えば、①表示装置６１ｂに表示されている原情報入力画面に入力ペンを用いて好みの数字、文字、記号、図形等を描く方法、②記録媒体に記憶されている原情報を情報読取装置により読み取る方法、③紙等に印刷されている画像を画像情報読取装置で読み取る方法等を用いることができる。図１６に示す実施例では、入力ペンを用いて原情報入力画面に「Ｅ」を描いた状態を示している。

次に、入力装置６１ｃを用いて、原情報を分割するための分割方法を指示する。原情報を分割する分割方法としては、種々の方法が可能である。例えば、原情報を分割線で分割する方法や、所定の論理式で分割する方法等を用いることができる。図１６に示す実施例では、入力ペンを用いて原情報入力画面に分割線（図１６の２点鎖線）を引いた状態を示している。

ユーザは、原情報を入力し、分割方法（この場合、分割線）を指示した後、分割処理を指示する。例えば、原情報入力画面に表示されている「入力終了」部を

選択する。端末装置６１は、分割処理が指示されると、原情報及び分割方法を管理装置５０に送信する。例えば、原情報入力画面上の原情報のビットパターン、表示画面上に引かれた分割線の表示画面上における位置情報を送信する。

管理装置５０は、端末装置６１の処理装置６１ａから送信された原情報及び分割方法を受信すると、入力された原情報を指示された分割方法で分割して、第１の情報(1)及び第２の情報(2)を形成する。この場合、管理装置５０は、分割線の位置情報を受信することにより、分割線で分割する分割方法が指示されたものと判断する。図１６に示す実施例では、原情報「Ｅ」を分割線で分割し、分割線で分割された「Ｅ」の左側の部分の情報を第１情報(1)（図１７参照）とし、分割線で分割された「Ｅ」の右側の部分の情報を第２情報(2)（図１７参照）とする。そして、形成した第１情報(1)及び第２情報(2)を端末装置６１に送信する。

端末装置６１の処理装置６１ａは、第１情報(1)及び第２情報(2)を受信すると、情報書込装置６１ｄに第１情報(1)、第２情報(2)及び原情報（この場合、入力画面上に描かれた「Ｅ」の情報）を出力する。

情報書込装置６１ｄは、第１情報(1)をユーザ携帯装置１０の記憶装置に書き込み、第２情報(2)及び原情報をユーザ装置２０の記憶装置に書き込む。

商品排出装置６１ｅは、第１情報が書き込まれたユーザ携帯装置１０、第２情報及び原情報が書き込まれたユーザ装置２０を商品排出口から排出する。

ユーザは、商品排出口から排出されたユーザ形態装置１０及びユーザ装置２０を受け取る。

商品排出口から排出するユーザ携帯装置１０及びユーザ装置２０は、ユーザが使用する用途に応じて種々の形態のものが用いられる。例えば、ユーザ携帯装置１０をユーザ携帯機器（腕時計、眼鏡、ベルト、イアリング、キーホルダ等）に取りつけて使用する場合には、微小な（例えば、数mm^2程度）四角形状のＩＣチップで形成し、取付手段によりユーザ携帯機器に取り付ける。取付手段としては、例えば、ＩＣチップの一方側の面に塗布された接着剤、クリップ、接着テープ等を用いることができる。ユーザ装置２０をユーザ機器（例えば、携帯電話機）４０に接続して使用する場合には、例えば、ユーザ機器（携帯電話機）４０に設けられているデータ入出力端子（接続端子）４９に接続可能な端子２９が設け

られているユーザ装置２０を用いる。

勿論、ユーザ携帯装置１０が一体に組み込まれているユーザ携帯機器（腕時計、眼鏡、ベルト、イアリング、キーホルダ等）や、ユーザ装置２０が一体に組み込まれているユーザ機器（キャッシュカード、デビットカード、携帯電話機、携帯端末等）を販売することも可能である。この場合には、ユーザ携帯装置１０をユーザ携帯機器に取り付ける作業や、ユーザ装置２０をユーザ機器に取り付ける作業が不要である。また、一体に形成されているため、取扱いが容易である。

ユーザ携帯装置１０やユーザ装置２０の形態は、端末装置毎に予め定めておいてもよいし、ユーザが本人確認装置を得る際に選択できるようにしてもよい。

なお、ユーザが本人確認装置の購入代金を支払うステップを設けてもよい。購入代金の支払方法は適宜選択可能である。

図１７に、本実施例の生成装置により生成されたユーザ携帯装置１０及びユーザ装置２０を示す。ユーザ携帯装置１０には、原情報「E」を分割して形成された第１情報(1)が記憶されている。ユーザ装置２０には、原情報「E」を分割して形成された第２情報(2)及び原情報「E」が記憶されている。

図１７に示すユーザ携帯装置１０は、ユーザ機器に接着剤等によって取り付けて使用したり、あるいはそのまま財布、ハンドバックやポケット等に入れて携帯するものである。

また、図１７に示すユーザ装置２０は、携帯電話機４０のデータ入出力端子（接続端子）４９に接続可能な接続端子２９が設けられている。この本人確認装置を使用する時には、ユーザ装置２０の接続端子２９と携帯電話機４０のデータ入力端子４９を接続する。これにより、ユーザ装置２０の処理装置（図示省略）と携帯電話機４０の処理装置４５との間の信号の伝送が可能となる。携帯電話機４０の処理装置４５は、例えば、ユーザ装置２０から出力禁止信号が出力されている時は、携帯電話機４０の使用を禁止する。

なお、図１６に示す実施例では、管理装置と端末装置により構成したが、端末装置自体に管理装置の機能を持たせることもできる。この場合には、端末装置単独で生成装置を構成することができる。また、表示装置６１ｂに表示された原情報を、表示装置６１ｂで指示された分割線に基づいて分割したが、原情報の入力

方法及び分割線の指示方法はこれに限定されない。さらに、分割線の数や引き方も図１６に示した方法に限定されない。また、原情報及び分割線を手で入力したが、原情報や分割線を予め複数用意しておき、その中から選択するようにしてもよい。この場合、原情報及び分割線の一方を手で入力するように構成すれば、分割情報が同一になる可能性は少ない。また、分割線に基づいて原情報を分割したが、原情報を分割する方法はこれに限定されない。また、商品排出装置を用いたが、商品排出装置は省略することもできる。また、端末装置６１～６３の設置場所は適宜変更可能である。また、ユーザ携帯装置やユーザ装置に情報を書き込む時の方法（手順）は、実施例で説明した方法に限定されず、種々の方法を用いることができる。

以上の実施例では、原情報を２つに分割したが、３以上に分割することもできる。原情報を３つに分割した場合の本人確認方法の実施例を図１８に示す。

本実施例では、本人確認処理（図１８の二点鎖線で囲んだ部分）が以下のように行われる。

本実施例では、本人確認装置は、第１ユーザ携帯装置１１０ａ、第２ユーザ携帯装置（１２０ａ及びユーザ装置１３０ａにより構成されている。第１ユーザ携帯装置１１０ａ及び第２ユーザ携帯装置１２０ａは、ユーザ１が携帯する腕時計（第１ユーザ携帯機器９１４０ａ及び眼鏡（第２ユーザ携帯機器）１５０ａに設けられている。ユーザ装置１３０ａは、ユーザが使用するデビットカード（ユーザ機器）１６０ａに設けられている。本実施例では、ユーザ装置１３０ａは、例えば、本人であることを確認できるまでは、使用禁止信号を出力してデビットカード１６０ａを使用不能状態とする。

元々一つの情報として認識される原情報を３つに分割し、第１の分割情報(1)を第１のユーザ携帯装置１１０ａに、第２の分割情報(2)を第２のユーザ携帯装置１２０ａに、第３の分割情報(3)をユーザ装置１３０ａに記憶させている。

なお、第１及び第２ユーザ携帯機器１４０ａ及び１５０ａは同じユーザ携帯機器を用いてもよい。また、第１及び第２のユーザ携帯装置１１０ａ及び１２０ａは、ユーザ携帯機器１４０ａ及び１５０ａと共に携帯する必要はなく、例えば、財布、カバンやポケットに入れて携帯してもよい。

第１及び第２ユーザ携帯装置１１０ａ及び１２０ａは、第１の情報(1)及び第２の情報(2)を送信する送信手段を備えている。

ユーザ装置１３０ａは、情報(1)及び情報(2)を受信すると、受信した情報(1)及び情報(2)と自身が記憶している第３の情報(3)を所定のアルゴリズムで結合して第４の情報(4)を形成する。そして、第４の情報(4)と原情報を照合することによって本人確認を行う。すなわち、受信した第１情報(1)と第２情報(2)と自身が記憶している情報(3)を結合して原情報を再生あるいは復元することができた場合に、本人であることを確認する。

図１９は、原情報を３つに分割した場合の本人確認方法における処理手順の例を説明する図である。本実施例では、ユーザ装置１３０は、常時本人確認処理を行う。本実施例では、①～⑤の手順で本人確認処理が行われる。

①ユーザ携帯装置１１０は、適宜の時期に第１情報(1)を送信する。

②ユーザ携帯装置１２０は、適宜の時期に第２情報(2)を送信する。

ここで、ユーザ携帯装置１１０及び１２０が同時に情報を送信すると、双方の情報が干渉してユーザ装置１３０で情報を正確に受信できなくなる可能性がある。そこで、ユーザ携帯装置１１０の送信時期とユーザ携帯装置１２０の送信時期が重ならないように設定するのが好ましい。例えば、ユーザ携帯装置１１０とユーザ携帯装置１２０が送信する時期を予め設定しておく。

③受信待機状態にあるユーザ装置１３０は、情報(1)及び情報(2)を受信する。

④ユーザ装置１３０は、受信した情報(1)及び情報(2)と自身が記憶している第３の情報(3)を所定のアルゴリズムで結合して第４の情報(4)を形成する。

⑤ユーザ装置１３０は、第４の情報(4)が原情報と一致した場合に、ユーザが本人であることを確認する。

図２０は、原情報を３つに分割した場合の本人確認方法における処理手順の他の例を説明する図である。本実施例では、ユーザ装置１３０は、本人確認が必要な場合に本人確認処理を行う。本実施例では、①～⑤の手順で本人確認処理が行われる。

①ユーザ装置１３０は、本人確認処理を行う必要がある場合に、送信要求信号を送信する。

②受信待機状態にあるユーザ携帯装置１１０は、送信要求信号を受信すると、自身が記憶している第１の情報(1)を送信する。

③受信待機状態にあるユーザ携帯装置１２０は、送信要求信号を受信すると、自身が記憶している第２の情報(2)を送信する。

ここで、ユーザ携帯装置１１０及び１２０が同時に情報を送信すると、双方の情報が干渉してユーザ装置１３０で情報を正確に受信できなくなる可能性がある。そこで、ユーザ携帯装置１１０の送信時期とユーザ携帯装置１２０の送信時期が重ならないように設定するのが好ましい。例えば、送信要求信号を受信してからそれぞれ異なる待機時間が経過した後に情報を送信するように設定する。

④受信待機状態にあるユーザ装置１３０は、受信した情報(1)及び情報(2)と自身が記憶している第３の情報(3)を所定のアルゴリズムで結合して第４の情報(4)を形成する。

⑤ユーザ装置１３０は、第４の情報(4)が原情報と一致する場合に、本人であることを確認する。

次に、原情報を３つに分割した分割情報を結合する例を図２１により具体的に説明する。

本実施例では、原情報［数字７の図形のビット行列］を、左右に引いた２本の分割線(1)及び分割線(2)を境に、上部の第１の情報(1)と、中央の第２の情報(2)と、下部の第３の情報(3)に分割している。そして、第１の情報(1)をユーザ携帯装置１１０に記憶させ、第２の情報(2)をユーザ携帯装置１２０に記憶させ、第３の情報(3)及び原情報をユーザ装置１３０に記憶させる。

ユーザ装置１３０は、受信した情報(1)及び(3)、自身が記憶している第３の情報(3)を所定のアルゴリズムで結合して第４の情報(4)を形成する。本実施例では、各情報のビット行列を結合する。そして、第４の情報(4)と原情報を照合して本人確認を行う。

本発明の本人確認装置の第７実施例のブロック図を図２２に示す。本実施例では、第１のユーザ携帯装置１１０ｂ、第２のユーザ携帯装置１２０ｂ及びユーザ装置１３０ｂにより構成されている。

第１のユーザ携帯装置１１０ｂは、信号出力装置１１１ｂ、変調／復調装置１

１２ｂ、通信装置１１３ｂにより構成されている。第２のユーザ携帯装置１２０ｂは、信号出力装置１２１ｂ、変調／復調装置１２２ｂ、通信装置１２３ｂにより構成されている。信号出力装置１１１ｂ、１２１ｂは、それぞれ第１の情報(1)、第２の情報(2)を記憶している。

ユーザ装置１３０ｂは、通信装置１３１ｂ、変調／復調装置１３２ｂ、結合装置１３３ｂ、信号出力装置１３４ｂにより構成されている。信号出力装置１３４ｂは、第３の情報(3)及び原情報を記憶する。結合装置１３３ｂは、受信した情報(1)及び第２情報(2)と、自身が記憶している第３の情報(3)を所定のアルゴリズムで結合して第４の情報(4)を形成する。そして、第４の情報(4)と原情報の照合結果に基づいて本人か否かを確認する。

以上の実施例では、原情報を３つに分割したが、原情報を４つ以上に分割することもできる。すなわち、本発明は、以下のように構成することができる。①原情報を分割して、Ｎ個（Ｎは２以上の整数）の分割情報を形成する。②第１分割情報～第（Ｎ－１）分割情報をそれぞれ第１ユーザ携帯装置～第（Ｎ－１）ユーザ携帯装置に記憶させるとともに、第Ｎ分割情報をユーザ装置に記憶させる。③ユーザ装置（本人確認手段）は、受信した情報と自身が記憶している情報を所定のアルゴリズムで結合し、原情報を形成することができた場合にユーザがそのユーザ機器の本来のユーザであることを確認する。

次に、暗号化機能を備えた本人確認装置の生成方法の一実施例を、図２３を参照して説明する。

図２３に示すように、まず、暗号装置８１、原コード記憶装置８２、暗号化コード記憶装置８３、接続線８４が設けられた回路基板Ｘを用意する。

暗号装置８１は、暗号化式を用いて原コードを暗号化し、あるいは暗号化された暗号化コードを復号化式を用いて復号化するものである。原コードとしては、種々の情報を用いることができる。本実施例では、暗号装置８１は、カオスジェネレータで生成されたカオス演算式を用いて暗号化式及び復号化式を決定し、暗号化式を用いて原コードを暗号化し、あるいは暗号化された暗号化コードを復号化式を用いて復号化する。カオスジェネレータは、時間的に変化するカオス演算式を発生する。ある時点でのカオス演算式は、原理的には初期値によって決定さ

れる。このカオス演算式を用いた暗号化式によって原コードを暗号化し暗号化コードは、カオス演算式の初期値がわからない場合には、ほとんど復号化することができない。カオスジェネレータは公知であるため、詳しい説明は省略する。

原コード記憶装置８２は、各時点における原コード（時間に対して一定の原コードを用いる場合と、時間に対して変化する原コードを用いる場合がある）、その時点に暗号装置８１で生成された復号化式を記憶する。

暗号化コード記憶装置８３は、各時点における、暗号装置８１で生成された暗号化式で原コードを暗号化した暗号化コードを記憶する。

暗号装置８１と暗号化コード記憶装置８３との間は、接続線８４で接続されている。接続線８４が切断されると、暗号化コード記憶装置８３への暗号化コードの記憶は停止される。すなわち、暗号化コード記憶装置８３には、回路基板Ｘが切断された時点における暗号装置８１の暗号化式によって原コードを暗号化した暗号化コードが記憶保持される。

回路基板Ｘには、回路基板Ｘを切断しやすいように、適当な個所に切断部が形成されている。本実施例では、回路基板Ｘの中央部に切り込み形成されている。回路基板Ｘには、切断部の両側に、第１回路基板Ｘ(1)及び第２回路基板Ｘ(2)が形成されている。

第１回路基板Ｘ(1)には、暗号装置８１及び原コード記憶装置８２が設けられている。第１回路基板Ｘ(1)には、情報の送受信をおこなうための、変調／復調装置や通信装置が設けられている。また、本人確認処理を実行するための本人確認装置が設けられている。暗号装置８１が本人確認装置を兼用してもよい。第１回路基板Ｘ(1)には、暗号装置８１等に電力を供給する電池が設けられている。

第２回路基板Ｘ(2)には、暗号化コード記憶装置８３が設けられている。第２回路基板Ｘ(2)には、情報の送受信をおこなうための、変調／復調装置や通信装置が設けられている。第２回路基板Ｘ(2)には、各装置に電力を供給する電池が設けられている。

本人確認装置を生成する場合には、任意の時間に、図２３に示す回路基板Ｘを切断部Ｘの部分で切断する。これにより、回路基板Ｘは、第１回路基板Ｘ(1)と第２回路基板に分割される。同時に、通信線８４が切断され、暗号装置８１と暗

号化コード記憶装置８３との接続が切断される。これにより、暗号化コード記憶装置８３には、切断時点における暗号装置８１の暗号化式で原コードを暗号化した暗号化コードが記憶保持される。

また、切断時点における原コード、切断時点における暗号装置８１の復号化式が原コード記憶装置８２に記憶保持される。

このようにして形成された第１回路基板Ｘ(1)及び第２回路基板Ｘ(2)は、一対の割符部材、すなわち本人確認装置を構成する。この場合、第１回路基板Ｘ(1)を受信側の割符部材（ユーザ装置）として用い、第２回路基板Ｘ(2)を送信側の割符部材（ユーザ携帯装置）として用いる。

例えば、第２回路基板Ｘ(2)を有するユーザ携帯装置は、暗号化コード記憶装置８３に記憶されている暗号化コードを送信する。一方、第１回路基板Ｘ(1)を有する受信側のユーザ装置は、受信した暗号化コードを、原コード記憶装置８２に記憶されている復号化式で復号化する。そして、復号化したコードが、原コード記憶装置８２に記憶されている原コードと一致した場合、自己と組になる割符部材であると判断する。すなわち、本人であることを確認する。

なお、信号の送受信を行うための通信装置や本人確認装置は、第１回路基板Ｘ(1)及び第２回路基板Ｘ(2)に設けてもよいし、第１回路基板Ｘ(1)及び第２回路基板Ｘ(2)を有するユーザ装置やユーザ携帯装置に設けてもよい。

図２４は、以上のようにして生成した本人確認装置を用いて認証システムを構成した図を示している。

図２４に示す実施例では、本人確認装置は、腕時計（ユーザ携帯機器）３０ｋに設けられたユーザ携帯装置１０ｋと、デビットカード（ユーザ機器）４０ｋに設けられたユーザ装置２０ｋにより構成されている。ユーザ携帯装置１０ｋには第２回路基板Ｘ(2)が設けられ、ユーザ装置２０ｋには第１回路基板Ｘ(1)が設けられている。

ユーザ携帯装置１０ｋは、記憶装置８３に記憶されている暗号化コードを送信する。ユーザ装置２０ｋは、暗号化コードを受信すると、受信した暗号化コードを、原コード記憶装置８２に記憶されている復号化式で復号化する。そして、復号化したコードが、原コード記憶装置８２に記憶されている原コードと一致した

場合に、本人であることを確認する。これにより、デビットカード４０ｋの使用が可能となる。

次に、図２４に示した本人確認装置の例を図２５に示す。

ユーザ携帯装置１０ｍは、信号出力装置１１ｍ、変調／復調装置１２ｍ、通信装置１３ｍにより構成されている。信号出力装置１１ｍは、暗号化コード記憶装置８３を有し、暗号化コードを出力する。

ユーザ装置２０ｍは、通信装置２１ｍ、変調／復調装置２２ｍ、本人確認装置２３ｍ、信号出力装置２４ｍを有している。信号出力装置２４ｍは、原コード記憶装置８２を有し、原コード及び復号化式を出力する。本人確認手段２３ｍは、受信した暗号化コードを、信号出力装置２４ｍから出力される復号化式で復号化する。そして、復号化したコードを、信号出力装置２４ｍから出力される原コードと照合して本人確認を行う。

図２４に示した本人確認装置の他の例を図２６に示す。図２６に示す実施例は、携帯電話機４０ｎをユーザ機器として用いている。また、ユーザ携帯装置１０ｎをポケットに入れて持ち運んでいる。

以上の実施例では、携帯装置で本人確認処理を行ったが、例えば認証センタで本人確認処理を行うこともできる。認証センタ等で本人確認処理を行う認証装置を用いた認証システムを図２７に示す。

本実施例では、公開鍵暗号化方式を用いて情報を送信することにより、情報の漏洩を防止している。公開鍵暗号化方式は、公知の暗号化方式であるため詳しい説明は省略するが、公開鍵と秘密鍵を用いる。公開鍵を用いて暗号化された情報は、公開鍵に対応する秘密鍵以外では復号化することができない。情報送信側は、情報受信側の公開鍵を用いて送信情報を暗号化して送信する。情報受信側では、受信した情報を自己の秘密鍵を用いて復号化する。この公開鍵暗号化方式を用いると、共通鍵暗号化方式のように秘密鍵を相手に知らせる必要がないため、秘密鍵が漏洩する恐れが少ない。また、情報受信側は、一つの公開鍵は用いることができるため、共通鍵暗号化方式に比べて鍵の数が少なくてすむ。

本実施例の本人確認装置は、腕時計（ユーザ携帯機器）３０ｐに設けられたユーザ携帯装置１０ｐと、デビットカード（ユーザ機器）４０ｐに設けられたユー

ザ装置２０ｐと、認証センタ１６０ｐとにより構成されている。

本実施例では、他の実施例と同様に、原情報を分割して第１の情報(1)と第２の情報(2)を形成し、第１の情報(1)をユーザ携帯装置１０ｐに記憶させ、第２の情報(2)をユーザ装置２０ｐに記憶させる。認証センタ１６０ｐの記憶手段（図示省略）には、各ユーザ機器４０ｐに設けられるユーザ装置２０ｐに記憶されている情報(2)の基となった原情報と、各ユーザ装置２０ｐで用いている公開鍵ＰＫに対応する秘密鍵ＳＫを各ユーザ装置２０ｐ（ユーザ機器４０ｐ）に対応させた記憶しているデータベースが記憶されている。

ユーザ携帯装置１０ｐは、自身が記憶している第１の情報(1)を送信する。ユーザ装置２０ｐは、受信した情報(1)と自身が記憶している第２の情報(2)を公開鍵を用いて暗号化し、認証端末装置１５０ｐを介して認証センタ１６０ｐに送信する。認証センタ１６０ｐは、ユーザ装置２０ｐから送信された情報を受信すると、記憶手段に記憶されているデータベースに基づいて、ユーザ装置２０ｐに対応する秘密鍵ＳＫを検索する。検索した秘密鍵ＳＫを用いて、受信した情報を復号化する。すなわち、ユーザ装置２０ｐが受信した情報(1)と、ユーザ装置２０ｐが記憶している情報（２）を抽出する。そして、復号化した情報(1)と情報(2)を結合して第３の情報(3)を形成し、第３の情報と原情報を照合して本人確認を行う。認証センタ１６０ｐは、本人を確認できた場合には、例えば、認証ＯＫ信号を認証端末装置１５０ｐに送信する。これにより、認証端末装置１５０ｐは、デビットカード４０ｐの使用を許可する。例えば、デビットカード４０ｐのカード情報の読み取りや暗証番号の入力を可能とする、あるいは代金の支払を可能とする。

ユーザ装置２０ｐから認証センタ１６０ｐに情報を送信する方法は、種々の方法が可能である。例えば、ユーザ機器が非接触式の通信装置（無線通信装置）を備えていないデビットカードである場合には、ユーザ機器と認証端末装置１５０ｐとの接続端子、認証端末装置１５０ｐ、通信回線１７０を介して認証センタ１６０ｐに至る伝送ルートＲ１を介して情報を認証センタ１６０ｐに送信する。ユーザ機器が無線通信装置を有する携帯電話機である場合には、無線通信回線、通信回線１７０を介して認証センタ１６０ｐに至る伝送ルートＲ２を介して情報を

認証センタ１６０ｐ送信する。ユーザ装置２０ｐが無線通信装置を有している場合には、無線通信回線、通信回線１７０を介して、ユーザ装置２０ｐから認証センタ１６０ｐに直接送信してもよい。

次に、公開鍵暗号化方式を用いた本人確認装置の例を図２８に示す。

ユーザ携帯装置１０ｑは、信号出力装置１１ｑ、変調／復調装置１２ｑ、通信装置１３ｑにより構成されている。信号出力装置１１ｑは、第１の情報(1)を記憶する記憶装置を有している。

ユーザ装置２０ｑは、通信装置２１ｑ、変調／復調装置２２ｑ、暗号化装置２３ｑ、信号出力装置２４ｑを有している。信号出力装置２４ｑは、第２の情報(2)と、情報を暗号化するときに用いる鍵（本実施例では、公開鍵ＰＫ）を記憶する記憶装置を有している。暗号化装置２３ｑは、受信した情報(1)と、信号出力装置２４ｑから出力される情報(2)を、信号出力装置２４ｑから出力される公開鍵ＰＫを用いて暗号化し、通信装置（図示省略）を介して外部（認証センタ１６０ｐ）に送信する。認証センタ１６０ｐに情報を送信する通信装置は、通信装置２１ｑを兼用してもよいし、ユーザ機器に設けられている通信装置を用いてもよい。

認証センタ１６０ｐは、ユーザ装置２０ｑから受信した情報を、当該情報を暗号化した公開鍵に対応する秘密鍵を用いて復号化する。そして、復号化した情報(1)と情報(2)を結合して原情報を形成することができた場合に、ユーザ１がそのユーザ機器の本来のユーザであることを確認する。

ユーザ装置２０ｑに公開鍵を記憶させる方法としては、種々の方法が可能である。例えば、予めユーザ装置２０ｑの信号出力装置２４ｑに記憶させておく方法を用いる。あるいは、本人確認処理を行う必要がある時または任意の時期に、認証センタ１６０ｐからユーザ装置２０ｑに送信する方法を用いる。あるいは、本人確認処理を行う必要がある時または任意の時期に、認証センタ１６０ｐが公開鍵を登録した第三者の認証機関から送信する方法を用いる。

次に、原情報を分割した分割情報を結合する方法の例を具体的に説明する。

図２９に示す例では、原情報［０１１１］を第１の情報(1)［００１１］と第２の情報(2)［０１０１］に分割している。そして、第１の情報(1)をユーザ携帯

装置１０に記憶させ、第２の情報(2)をユーザ装置２０に記憶させている。原情報は、認証センタ６０の記憶装置に記憶させている。

ユーザ装置２０は、受信した情報(1)と、自身が記憶している情報(2)を、所定の公開鍵ＰＫで暗号化（『ＰＫ（情報(1)）』、『ＰＫ（情報(2)）』）して、認証センタ６０に送信する。

認証センタ６０は、ユーザ装置２０から受信した情報（『ＰＫ（情報(1)）』、『ＰＫ（情報(2)）』）を、ユーザ装置２０で使用した公開鍵ＰＫに対応する秘密鍵ＳＫで復号化（『ＳＫ[ＰＫ（情報(1)）]』、『ＳＫ[ＰＫ（情報(2)）]』）して情報(1)及び情報(2)を得る。

さらに、復号化した情報(1)及び情報(2)を所定のアルゴリズムで結合して第３の情報(3)を形成する。次いで、情報(3)と原情報とを照合して本人確認を行う。

図３０に示す例では、原情報［数字７の図形のビット行列］を、図３０で左右に引いた分割線を境に、上部の第１の情報(1)と下部の第２の情報(2)に分割する。そして、第１の情報(1)をユーザ携帯装置１０に記憶させ、第２の情報(2)をユーザ装置２０に記憶させる。原情報は、認証センタ６０ａの記憶装置に記憶させる。

ユーザ装置２０は、受信した情報(1)と、自身が記憶している情報(2)を、所定の公開鍵ＰＫで暗号化（『ＰＫ（情報(1)）』、『ＰＫ（情報(2)）』）して、認証センタ１６０に送信する。

認証センタ１６０は、ユーザ装置２０から受信した情報（『ＰＫ（情報(1)）』、『ＰＫ（情報(2)）』）を、ユーザ装置２０で使用した公開鍵ＰＫに対応する秘密鍵ＳＫを用いて復号化（『ＳＫ[ＰＫ（情報(1)）]』、『ＳＫ[ＰＫ（情報(2)）]』）して情報(1)及び情報(2)を得る。

さらに、復号化した情報(1)及び情報(2)を所定のアルゴリズムで結合して情報(3)を形成する。さらに、情報(3)と原情報を照合して本人確認を行う。

上記実施例では、ユーザ装置に公開鍵を記憶させたが、公開鍵も分割してユーザ携帯装置とユーザ装置に記憶させることにより、より信頼性を高めることができる。公開鍵を分割して記憶させる実施例を図３１に示す。

図３１に示す実施例では、原情報を分割して形成した第１の情報(1)をユーザ

携帯装置１０ｒに記憶させ、第２の情報(2)をユーザ装置２０ｒに記憶させている。さらに、所定の公開鍵ＰＫを分割して第１の公開鍵ＰＫ(1)及び第２の公開鍵ＰＫ(2)を形成する。そして、第１の公開鍵ＰＫ(1)をユーザ携帯装置１０ｒに記憶させ、第２の公開鍵ＰＫ(2)をユーザ装置２０ｒに記憶させる。

ユーザ携帯装置１０ｒは、第１の情報(1)及び第１の公開鍵(1)を送信する。

ユーザ装置２０ｒの暗号化装置２３ｒは、受信した公開鍵ＰＫ(1)と自身が記憶している公開鍵ＰＫ(2)を所定のアルゴリズムで結合して公開鍵ＰＫを形成する。所定のアルゴリズムは、公開鍵ＰＫの分割方法によって決定される。そして、受信した情報(1)と自身が記憶している情報(2)を、公開鍵ＰＫ(1)及びＰＫ(2)を結合して形成した公開鍵ＰＫを用いて暗号化し、認証センタ１６０ｐに送信する。

認証センタ１６０ｐは、受信した情報をユーザ装置２０ｒが用いている公開鍵ＰＫに対応する秘密鍵ＳＫを用いて復号化する。そして、復号化した情報と原情報を照合して本人確認を行う。

本実施例では、情報(1)及び公開鍵ＰＫ(1)の双方が正しくないと、本人であると確認されないため、信頼性が高くなる。

ユーザ機器として携帯電話機を用い、公開鍵暗号化方式を用いて情報を送信する本人確認装置を図３２に示す。

本実施例では、ユーザ携帯装置１０ｓは、ユーザ１の胸ポケットに入れて携帯している。また、ユーザ装置２０ｓは、携帯電話機４０ｓ（ユーザ機器）に取りつけられている。ユーザ装置２０ｓに、携帯電話機４０ｓのデータ入出力端子と接続可能な接続端子を設けると、ユーザ装置２０ｓと携帯電話機４０ｓとの接続作業が容易となる。

以上の説明では、ユーザ携帯装置とユーザ装置との間の情報の送受信を非接触で行ったが、接触させた状態で情報の送受信をおこなうこともできる。例えば、ユーザ携帯機器としての磁気的あるいは電気的なＩＤカード、ＩＤカードタグ、携帯電話機を、ユーザ機器としてのパソコンのカード挿入口に差込みあるいはケーブルで接続しても良い。この場合、ＩＤカードあるいは携帯電話機から第１情報をパソコンに送信する。パソコンは、受信した情報と自己が保有する情報とを

結合して原情報を形成することができた場合には、パソコンの使用を許可する。あるいは、逆に、パソコンをユーザ携帯装置、ＩＤカードや携帯電話機をユーザ機器として用いることもできる。

本発明は、以下に記載する効果を有する。

本発明は、生体情報、暗証番号、サイン（署名）、印章あるいはＩＤコード等を用いるのでなく、割り符のような、元々は一つの情報または信号を分割した情報を用いている。そして、各分割情報を、ユーザが携帯するユーザ携帯装置とユーザが使用するユーザ機器に設けられるユーザ装置にそれぞれ記憶させ、ユーザ携帯装置とユーザ装置が記憶している情報を結合した情報に基づいて本人確認を行っている。このような情報は、生体情報のように変動することがない。また、通信手段や各情報の結合手段等は、ＩＣチップ等によって簡単に、安価に構成することができる。したがって、精度が高く、かつ低コストで本人確認を行うことができる。

また、本発明では、ユーザ携帯装置が記憶している情報とユーザ装置が記憶している情報が結合されて原情報が復元されない限り、本人確認が行われない。このため、暗証番号、カードやＩＤタグ等を盗まれても不正使用の心配がない。つまり、ユーザ装置及びユーザ携帯装置を落としたり、盗まれたりしない限り、不正使用の恐れはない。ユーザ携帯装置をＩＣチップで構成すれば、ユーザが携帯可能な多くの部材（例えば、指輪やメガネ）に取り付けることができる。この場合、ユーザ携帯装置を、ユーザが自分で決めた部材に取り付けることができるので、ユーザ携帯機器が盗まれる恐れもほとんどない。万一、情報が漏れている恐れがある場合には、ユーザ携帯装置及びユーザ装置の所定のＩＣチップを新たなチップに交換すればよい。

以上のように、本発明を用いることにより、不特定多数のユーザに対して、簡単、低コスト、高信頼性、高セキュリティで本人確認処理を行うことができる。

本発明は、前記した実施例の構成に限定されることなく、本発明の要旨を変更しない範囲で種々の変更、追加、削除が可能である。例えば、ユーザ装置とユーザ機器との組付け形態、ユーザ携帯装置とユーザ携帯機器との組付け形態は、一体構成あるいは別体構成等種々変更可能である。

請 求 の 範 囲

1．ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認方法であって、

原情報を第１情報と第２情報に分割し、第１情報をユーザが携帯するユーザ携帯装置に記憶させるとともに、第２情報をユーザが使用するユーザ機器に設けられるユーザ装置に記憶させるステップと、

ユーザ携帯装置から第１情報を送信するステップと、

ユーザ装置で情報を受信するステップと、

ユーザ装置で受信した情報とユーザ装置が記憶している第２情報を結合し、原情報を形成することができた場合に本人であることを確認するステップと、

を備えることを特徴とする本人確認方法。

2．請求項１に記載の本人確認方法であって、

ユーザ携帯装置から第１情報を送信するステップでは、第１情報を暗号化して送信し、

ユーザ装置で情報を受信するステップでは、受信した情報を復号化する、

ことを特徴とする本人確認方法。

3．請求項１に記載の本人確認方法であって、

ユーザ携帯装置から第１情報を送信するステップでは、第１情報にランダムノイズを挿入し、

ユーザ装置で情報を受信するステップでは、受信した情報からランダムノイズを除去する、

ことを特徴とする本人確認方法。

4．請求項１に記載の本人確認方法であって、

ユーザ携帯装置から第１情報を送信するステップでは、第１情報を無線で送信する、

ことを特徴とする本人確認方法。

5．請求項１に記載の本人確認方法であって、更に、

ユーザ装置から情報送信要求信号を送信するステップを備え、

ユーザ携帯装置から第１情報を送信するステップでは、ユーザ携帯装置が情報

送信要求信号を受信した時に第１情報を送信する、

ことを特徴とする本人確認方法。

６．ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認装置であって、

ユーザが携帯するユーザ携帯装置と、

ユーザが使用するユーザ機器に設けられるユーザ装置とを備え、

ユーザ携帯装置は、原情報を分割して形成した第１情報と第２情報のうちの第１情報を記憶する第１記憶装置と、第１記憶装置に記憶されている第１情報を変調する変調装置と、第１通信装置とを有し、

ユーザ装置は、原情報を分割して得た第１情報と第２情報のうち第２情報を記憶する第２記憶装置と、第２通信装置と、第２通信装置で受信した情報を復調する復調装置と、復調装置で復調した情報と第２記憶装置に記憶している第２情報を結合して原情報を形成することができた場合に本人であることを確認する本人確認装置とを有する、

ことを特徴とする本人確認装置。

７．請求項６に記載の本人確認装置であって、

ユーザ携帯装置は、所定時間毎に第１情報を送信する、

ことを特徴とする本人確認装置。

８．請求項６に記載の本人確認装置であって、

ユーザ装置は、本人確認が必要な時に情報送信要求信号を送信し、

ユーザ携帯装置は、情報送信要求信号を受信した時に第１情報を送信する、

ことを特徴とする本人確認装置。

９．請求項６に記載の本人確認装置であって、

ユーザ携帯装置は、第１情報を暗号化する暗号化装置を有し、

ユーザ装置は、受信した情報を復号化する復号化装置を有する、

特徴とする本人確認装置。

１０．請求項６に記載の本人確認装置であって、

ユーザ携帯装置は、第１情報にランダムノイズを挿入するランダムノイズ挿入装置を有し、

ユーザ装置は、受信した情報からランダムノイズを除去するランダムノイズ除去装置を有する、

ことを特徴とする本人確認装置。

１１．請求項６に記載の本人確認装置であって、

ユーザ装置は、更に、不正に第２情報が読み出されることを検出した時に第２記憶装置に記憶されている第２情報の読み出しを禁止する読出禁止装置を有する、

ことを特徴とする本人確認装置。

１２．請求項１１に記載の本人確認装置であって、読出禁止装置は第２記憶装置を破壊する、本人確認装置。

１３．請求項６に記載の本人確認装置であって、ユーザ携帯装置及びユーザ装置の少なくとも一方はＩＣチップを含んでいる、ことを特徴とする本人確認装置。

１４．請求項１３に記載の本人確認装置であって、ＩＣチップが交換可能に設けられている、ことを特徴とする本人確認装置。

１５．請求項６に記載の本人確認装置であって、ユーザ機器がカード状部材である、ことを特徴とする本人確認装置。

１６．請求項６に記載の本人確認装置であって、ユーザ機器が決済用カードであり、本人確認装置は、本人であることを確認した場合に決済用カードに記憶されているカード情報の読み出しを許可する、ことを特徴とする本人確認装置。

１７．請求項６に記載の本人確認装置であって、ユーザ機器が通信機である、ことを特徴とする本人確認装置。

１８．請求項１７に記載の本人確認装置であって、本人確認装置は、本人であることを確認した場合に通信機の使用を許可する、ことを特徴とする本人確認装置。

１９．請求項６に記載の本人確認装置の生成装置であって、ユーザ装置には、ユーザ機器の接続端子と接続可能な接続端子が設けられている、ことを特徴とする本人確認装置。

２０．ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認装置であって、

ユーザが携帯するＮ個（Ｎは３以上の整数）のユーザ携帯装置と、

ユーザが使用するユーザ機器に設けられるユーザ装置とを備え、

第１～第（Ｎ－１）のユーザ携帯装置は、それぞれ第１～第Ｎ記憶装置と、第１～第（Ｎ－１）記憶装置に記憶されている情報を送信する第１～第（Ｎ－１）通信装置とを有し、

ユーザ装置は、第Ｎ記憶装置と、第Ｎ通信装置と本人確認装置を備え、

第１～第（Ｎ－１）記憶装置は、原情報を分割して形成した第１～第Ｎの情報のうちの第１～（Ｎ－１）情報を記憶し、

第Ｎ記憶装置は、原情報を分割して形成した第１～第Ｎの情報のうちの第Ｎの情報を記憶し、本人確認装置は、通信装置で受信した情報と第Ｎ記憶装置に記憶されている情報を結合し、原情報を形成することができた場合に本人であることを確認する、

ことを特徴とする本人確認装置。

２１．ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認方法であって、

原情報を第１情報と第２情報に分割し、第１情報をユーザが携帯するユーザ携帯装置に記憶させ、第２情報をユーザが使用するユーザ機器に設けられるユーザ装置に記憶させるステップと、

ユーザ携帯装置から第１情報を送信するステップと、

ユーザ装置で第１情報を受信するステップと、

ユーザ装置で受信した第１情報とユーザ装置が記憶している第２情報をユーザ装置から認証センタに送信するステップと、

認証センタで、ユーザ装置から送信された第１情報及び第２情報を受信するステップと、

認証センタで受信した第１情報と第２情報を結合して、原情報を作成することができた場合に本人であることを確認するステップと、

を備えることを特徴とする本人確認方法。

２２．請求項２１に記載の本人確認方法であって、

ユーザ装置で受信した第１情報とユーザ装置が記憶している第２情報をユーザ

装置から認証センタに送信するステップでは、ユーザ装置で受信した第１情報とユーザ装置が記憶している第２情報を公開鍵で暗号化して認証センタに送信し、

認証センタで第１情報及び第２情報を受信するステップでは、受信した情報を、ユーザ装置で用いている公開鍵に対応する秘密鍵を用いて復号化する、

ことを特徴とする本人確認方法。

２３．ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認方法であって、

原情報を第１情報と第２情報に分割し、第１情報をユーザが携帯するユーザ携帯装置に記憶させ、第２情報をユーザが使用するユーザ機器に設けられるユーザ装置に記憶させるステップと、

公開鍵を第１公開鍵と第２公開鍵に分割し、第１公開鍵をユーザ携帯装置に記憶させ、第２公開鍵をユーザ装置に記憶させるステップと、

ユーザ携帯装置から第１情報及び第１公開鍵を送信するステップと、

ユーザ装置で第１情報及び第１公開鍵を受信するステップと、

ユーザ装置で受信した第１情報とユーザ装置が記憶している第２情報を、ユーザ装置で受信した第１公開鍵とユーザ装置が保有している第２公開鍵を結合した公開鍵を用いて暗号化して認証センタに送信するステップと、

認証センタで暗号化情報を受信するステップと、

認証センタで受信した暗号化情報を、ユーザ装置で用いられている公開鍵に対応する秘密鍵を用いて第１情報と第２情報を復号化し、復号化した第１情報と第２情報を結合し、原情報を作成することができた場合に本人であることを確認するステップと、

を備えることを特徴とする本人確認方法。

２４．ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認装置であって、

ユーザが携帯するユーザ携帯装置と、

ユーザが使用するユーザ機器に設けられるユーザ装置と、

認証センタとを備え、

ユーザ携帯装置は、原情報を分割して得た第１情報と第２情報のうちの第１情

報を記憶する第１記憶装置と、第１記憶装置に記憶されている第１情報を送信する第１通信装置とを有し、

ユーザ装置は、原情報を分割して得た第１情報と第２情報のうちの第２情報を記憶する第２記憶装置と、第２通信装置と、第２通信装置で受信した第１情報と第２記憶装置に記憶している第２情報を認証センタに送信する第３通信装置とを有し、

認証センタは、ユーザ装置から送信された第１情報と第２情報を結合して、原情報を形成することができた場合に本人であることを確認する本人確認装置を有する、

ことを特徴とする本人確認装置。

２５．請求項２４に記載の本人確認装置であって、

ユーザ携帯装置は、第２通信装置で受信した第１情報と第２記憶装置に記憶されている第２情報を暗号化する暗号化装置を有し、

認証センタは、ユーザ装置から送信された暗号化情報を復号化する復号化装置を有する、

ことを特徴とする本人確認装置。

２６．請求項２５に記載の本人確認装置であって、

暗号化装置は、公開鍵を用いて暗号化を行い、

復号化装置は、公開鍵に対応する秘密鍵を用いて復号化を行う、

ことを特徴とする本人確認装置。

２７．ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認装置であって、

ユーザが携帯するユーザ携帯装置と、

ユーザが使用するユーザ機器に設けられるユーザ装置と、

認証センタとを備え、

ユーザ携帯装置は、原情報を分割して形成した第１情報と第２情報のうちの第１情報及び公開鍵を分割して形成した第１公開鍵と第２公開鍵のうちの第１公開鍵を記憶する第１記憶装置と、第１記憶装置に記憶されている第１情報及び第１公開鍵を送信する第１通信装置とを有し、

ユーザ装置は、原情報を分割して形成した第１情報と第２情報のうちの第２情報及び公開鍵を分割して得た第１公開鍵と第２公開鍵のうちの第２公開鍵を記憶する第２記憶装置と、第２通信装置と、第２通信装置で受信した第１情報と第２記憶手段に記憶している第２情報を、第２通信装置で受信した第１公開鍵と第２記憶手段に記憶している第２公開鍵を結合して形成した公開鍵を用いて暗号化して認証センタに送信する第３通信装置とを有し、

認証センタは、ユーザ装置から送信された暗号化情報を、ユーザ装置で用いられている公開鍵に対応する秘密鍵を用いて復号化し、復号化された第１情報と第２情報を結合し、原情報を形成することができた場合に本人であることを確認する本人確認装置を有する、

ことを特徴とする本人確認装置。

２８．ユーザが携帯し、原情報を分割して形成した第１情報と第２情報のうちの第１情報を記憶する第１記憶装置と、第１記憶装置に記憶されている第１情報を送信する第１通信装置を有するユーザ携帯装置と、ユーザが使用するユーザ機器に設けられ、原情報を分割して形成した第１情報と第２情報のうちの第２情報を記憶する第２記憶装置と、第２通信装置と、第２通信装置により受信した情報と第２情報を結合して原情報を形成することができた場合に本人であることを確認する本人確認装置を有するユーザ装置とにより構成される本人確認装置の生成装置であって、

処理装置と、情報書込装置と、表示装置とを備え、

処理装置は、表示装置に表示されている原情報を、表示装置に表示されている分割線に基づいて分割して第１情報及び第２情報を形成し、形成した第１情報及び第２情報を情報書込装置に出力し、

情報書込装置は、処理装置から出力された第１情報をユーザ携帯装置の第１記憶装置に書き込むとともに、処理装置から出力された第２情報をユーザ装置の第２記憶装置に書き込む、

ことを特徴とする本人確認装置の生成装置。

２９．ユーザが携帯し、原情報を分割して形成した第１情報と第２情報のうちの第１情報を記憶する第１記憶装置と、第１記憶装置に記憶されている第１情報を

送信する第１通信装置を有するユーザ携帯装置と、ユーザが使用するユーザ機器に設けられ、原情報を分割して形成した第１情報と第２情報のうちの第２情報を記憶する第２記憶装置と、第２通信装置と、第２通信装置により受信した情報と第２情報を結合して原情報を形成することができた場合に本人であることを確認する本人確認装置を有するユーザ装置とにより構成される本人確認装置の生成装置であって、

処理装置と、情報書込装置と、入力装置とを備え、

処理装置は、入力装置より入力された原情報を、入力装置により指示された分割方法で分割して第１情報と第２情報を形成し、形成した第１情報及び第２情報を情報書込装置に出力し、

情報書込装置は、処理装置から出力された第１情報をユーザ携帯装置の第１記憶装置に書き込むとともに、処理装置から出力された第２情報をユーザ装置の第２記憶装置に書き込む、

ことを特徴とする本人確認装置の生成装置。

３０．請求項２９に記載の本人確認装置の生成装置であって、

更に、商品排出装置を備え、

商品排出装置は、情報書込装置によって第１情報が書き込まれたユーザ携帯装置及び第２情報が書き込まれたユーザ装置を商品排出口から排出する、

ことを特徴とする本人確認装置の生成装置。

３１．第１情報を送信する第１の装置と、第１の装置から受信した第１の情報と自身が記憶している第２の情報を結合し、所定の情報を形成することができた場合に本人であることを確認する本人確認装置の生成方法であって、

暗号化式及び復号化式を生成し、暗号化式を用いて暗号化を行い、復号化式を用いて復号化を行う暗号装置と、暗号装置によって生成された暗号化式を用いて原コードを暗号化した暗号化コードを記憶する暗号化コード記憶装置と、暗号装置によって生成された復号化式と原コードを記憶する原コード記憶装置を有する回路基板を用意するステップと、

回路基板を切断して、暗号装置と原コード記憶装置を有する第１回路基板と、暗号化コード記憶装置を有する第２回路基板を形成するステップと、

第１回路基板を第２の装置に用い、第２回路基板を第１の装置に用いるステップと、

を備えることを特徴とする本人確認装置の生成方法。

３２．請求項３１に記載の本人確認装置の生成方法であって、

暗号装置は、時間的に変化する暗号化式及び復号化式を生成するものであり、

暗号化コード記憶装置には、回路基板切断時の暗号化式を用いて原コードを暗号化した暗号化コードが記憶保持され、

原コード記憶装置には、回路基板切断時の復号化式と原コードが記憶されている、

ことを特徴とする本人確認装置の生成方法。

３３．請求項３２に記載の本人確認装置の生成方法であって、

暗号装置は、カオスジェネレータで生成されたカオス演算式を用いて暗号化及び復号化を行う、

ことを特徴とする本人確認装置の生成方法。

３４．請求項３１に記載の本人確認装置の生成方法であって、回路基板を切断するステップでは、回路基板に形成されている切断部の個所を切断する、ことを特徴とする本人確認装置の生成方法。

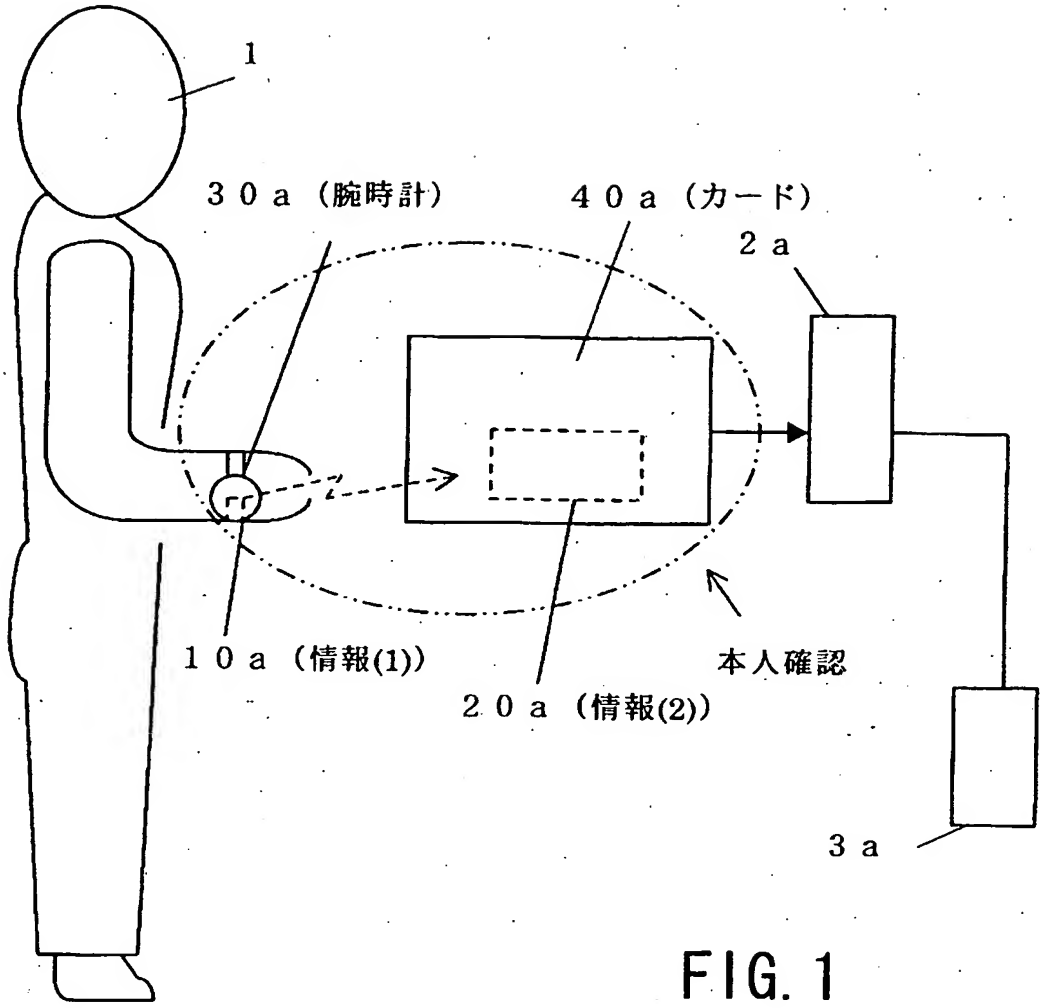

1
３０ａ（腕時計）
４０ａ（カード）
２ａ
１０ａ（情報(1)）
２０ａ（情報(2)）
本人確認
３ａ

FIG. 1

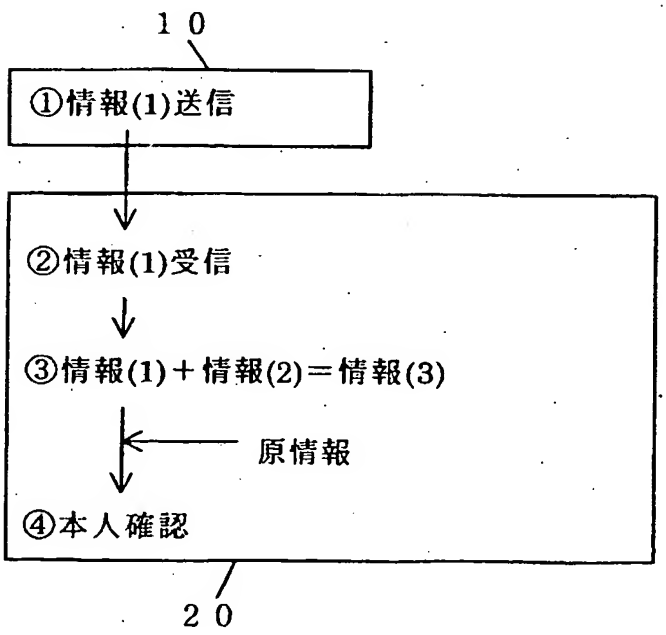

１０
①情報(1)送信
②情報(1)受信
③情報(1)＋情報(2)＝情報(3)
原情報
④本人確認
２０

FIG. 2

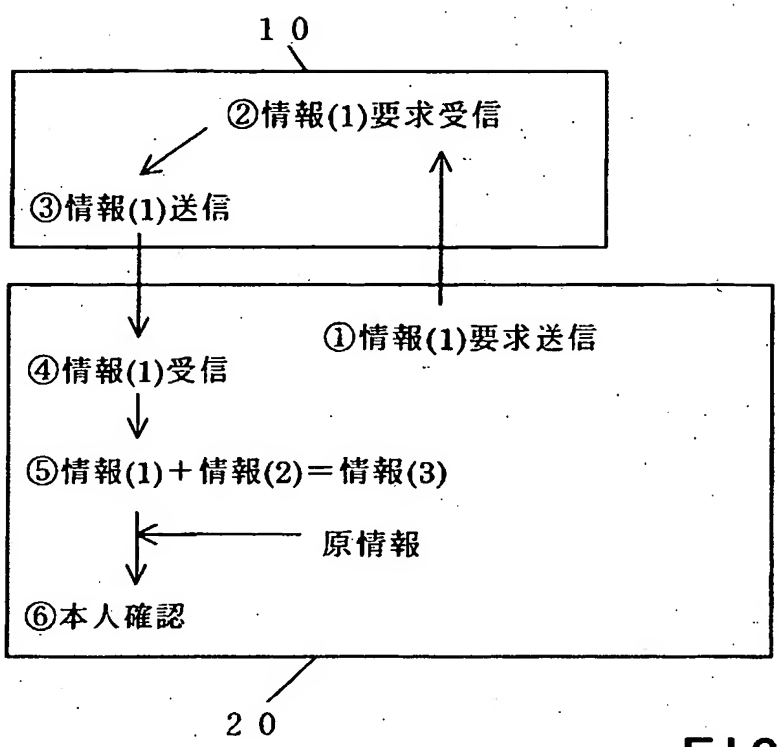

10
②情報(1)要求受信
③情報(1)送信
①情報(1)要求送信
④情報(1)受信
⑤情報(1)＋情報(2)＝情報(3)
原情報
⑥本人確認
20

FIG. 3

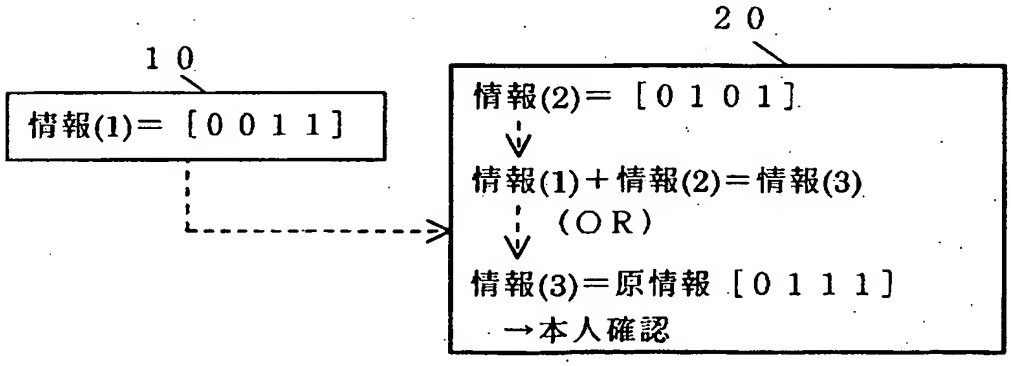

20
10
情報(1)＝［0011］
情報(2)＝［0101］
情報(1)＋情報(2)＝情報(3)
（OR）
情報(3)＝原情報［0111］
→本人確認

FIG. 4

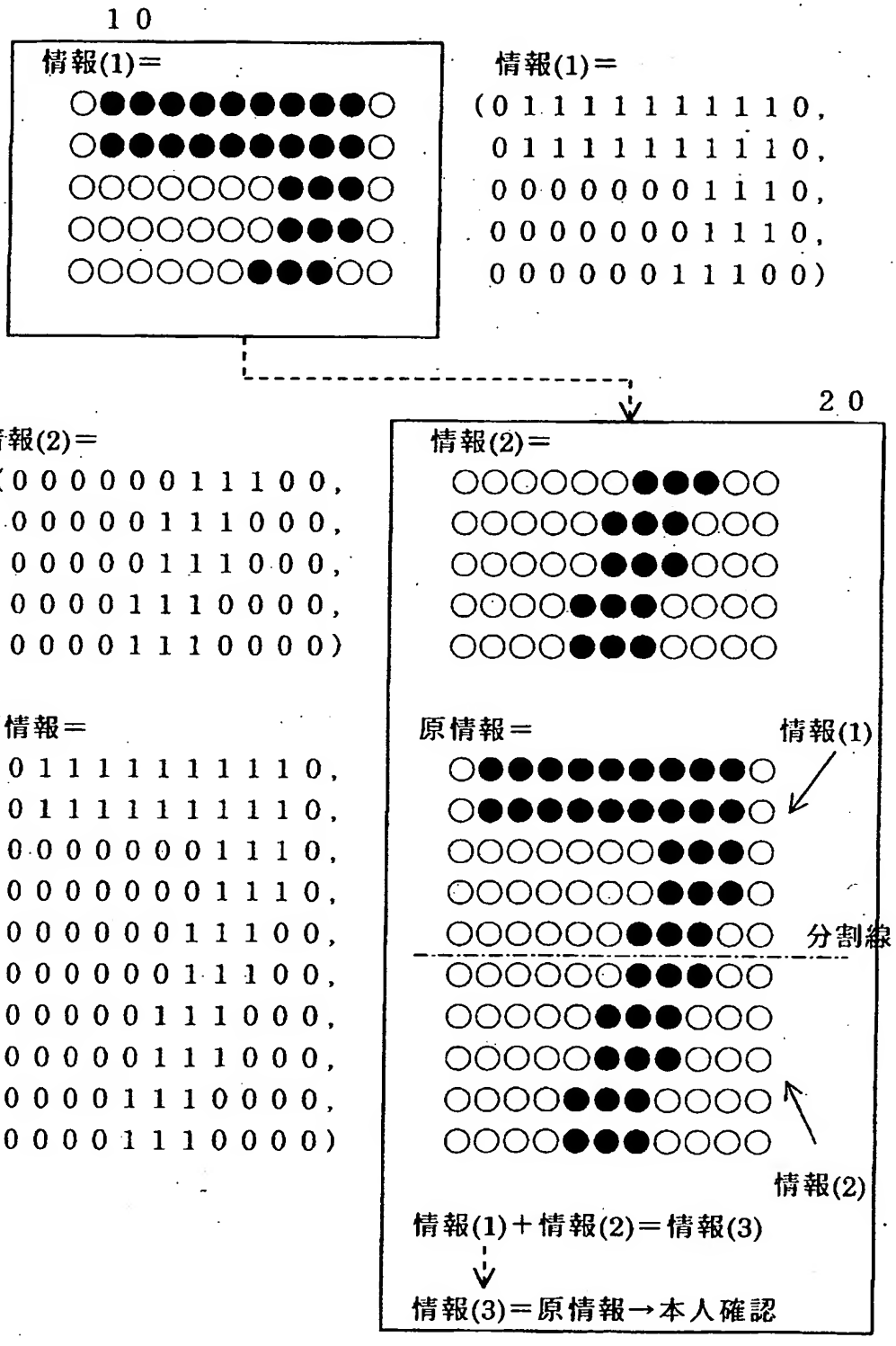

10
情報(1)＝
(0111111111110,
0111111111110,
0000000011110,
0000000001110,
0000000111100)
20
情報(2)＝
(0000000111100,
0000011110000,
0000011110000,
0000111100000,
0000111100000)
情報(2)＝
原情報＝
(0111111111110,
0111111111110,
0000000011110,
0000000001110,
0000000111100,
0000000111100,
0000011110000,
0000011110000,
0000111100000,
0000111100000)
原情報＝
情報(1)
分割線
情報(2)
情報(1)＋情報(2)＝情報(3)
情報(3)＝原情報→本人確認

FIG. 5

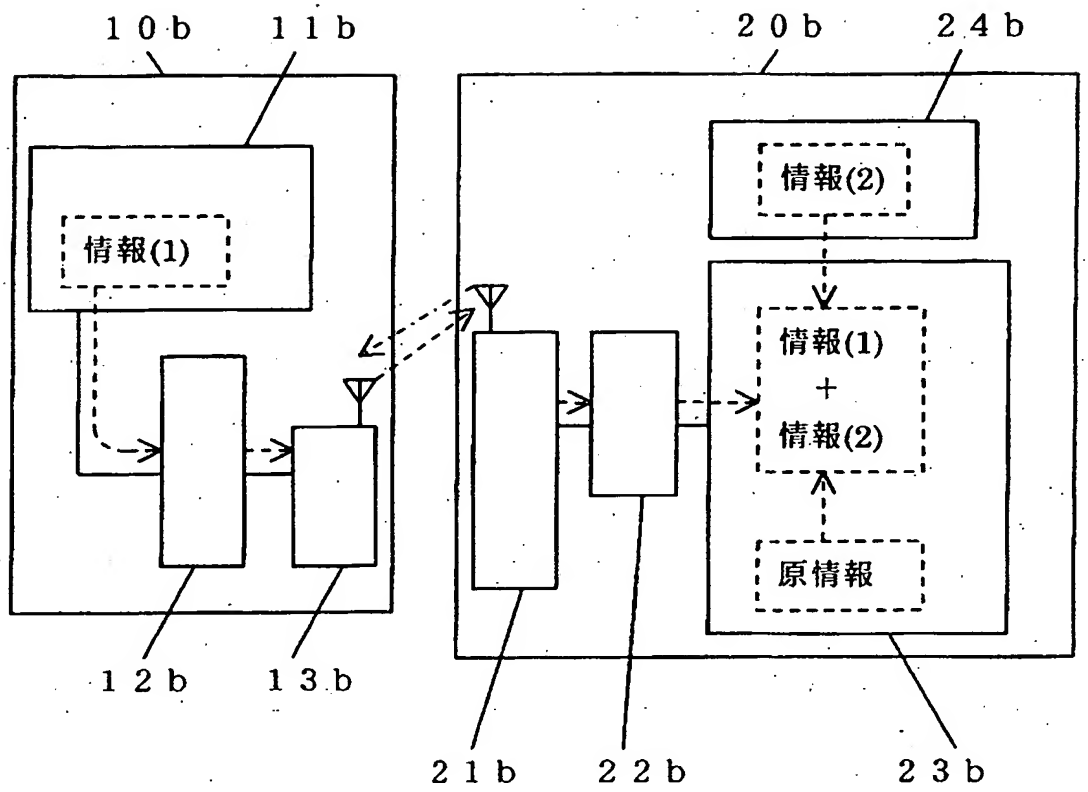

10b
11b
20b
24b
情報(1)
情報(2)
情報(1)
+
情報(2)
原情報
12b
13b
21b
22b
23b

FIG. 6

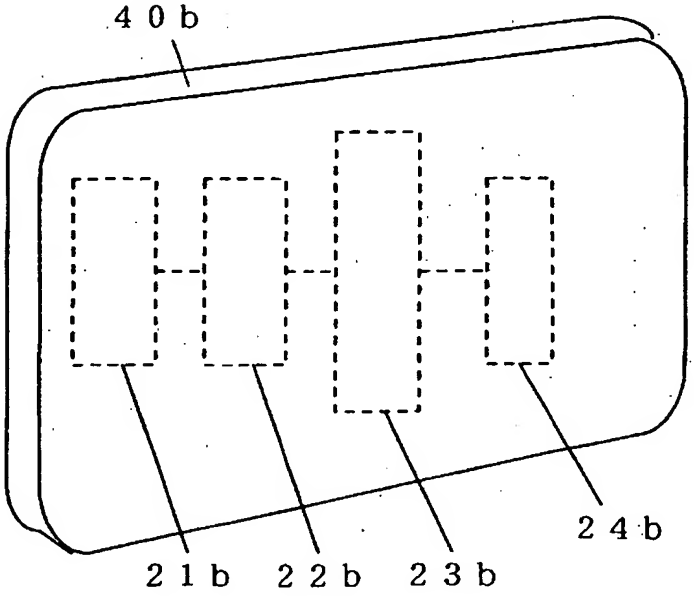

40b
21b
22b
23b
24b

FIG. 7

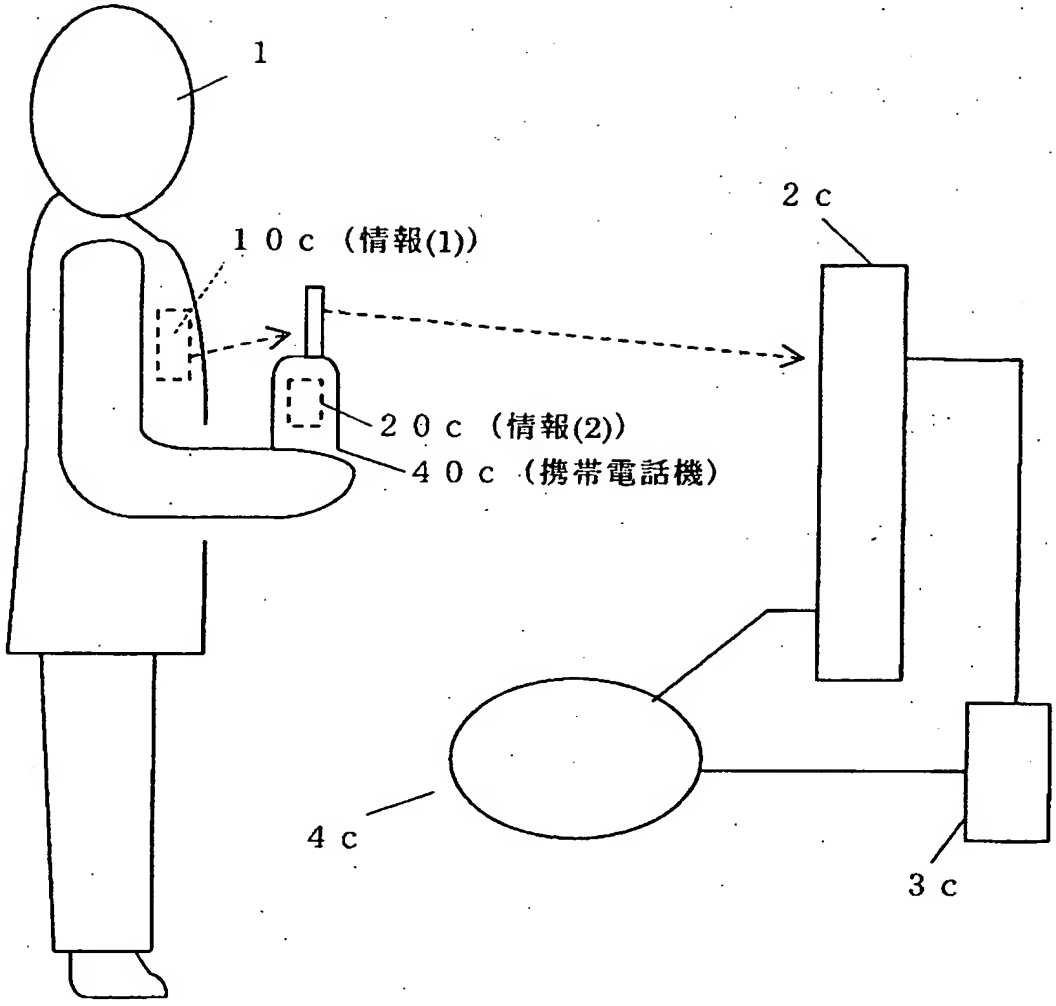


FIG. 8

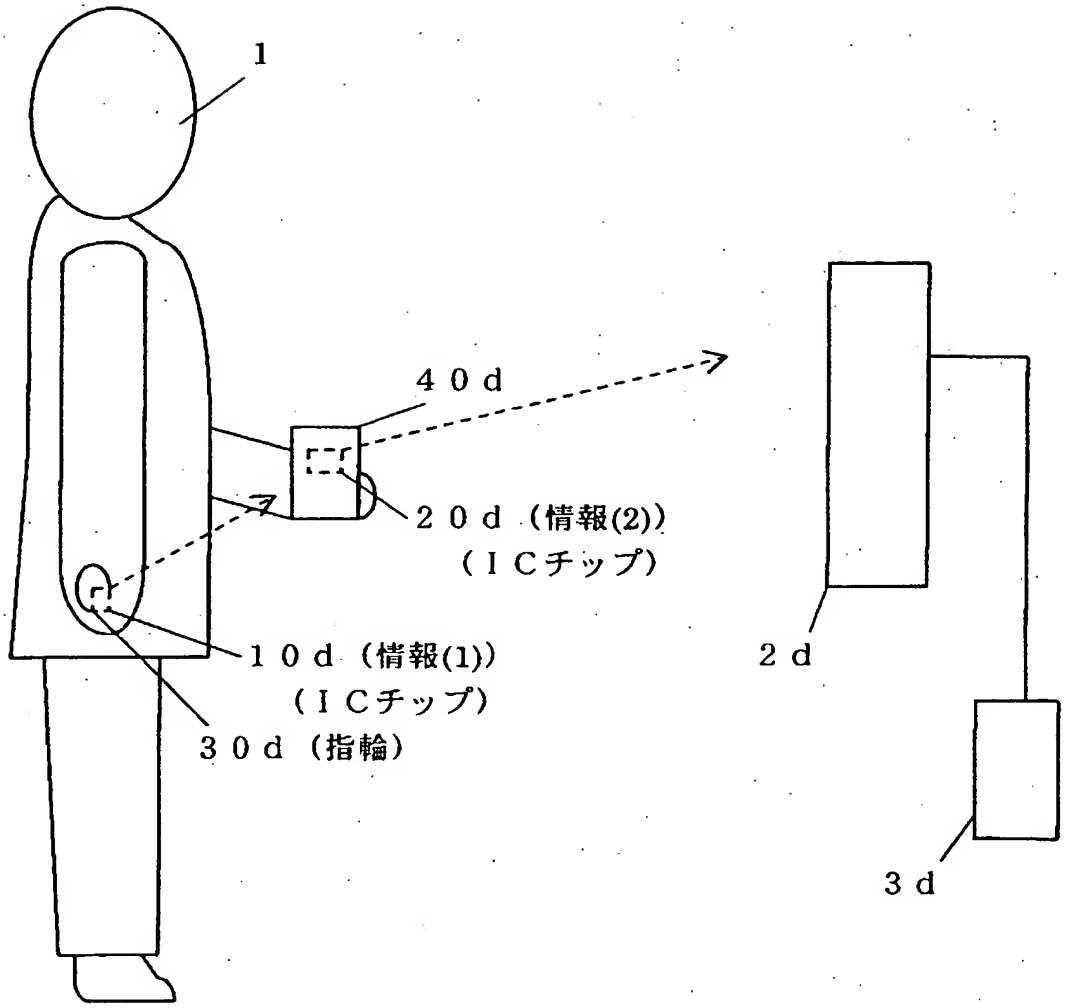


FIG. 9

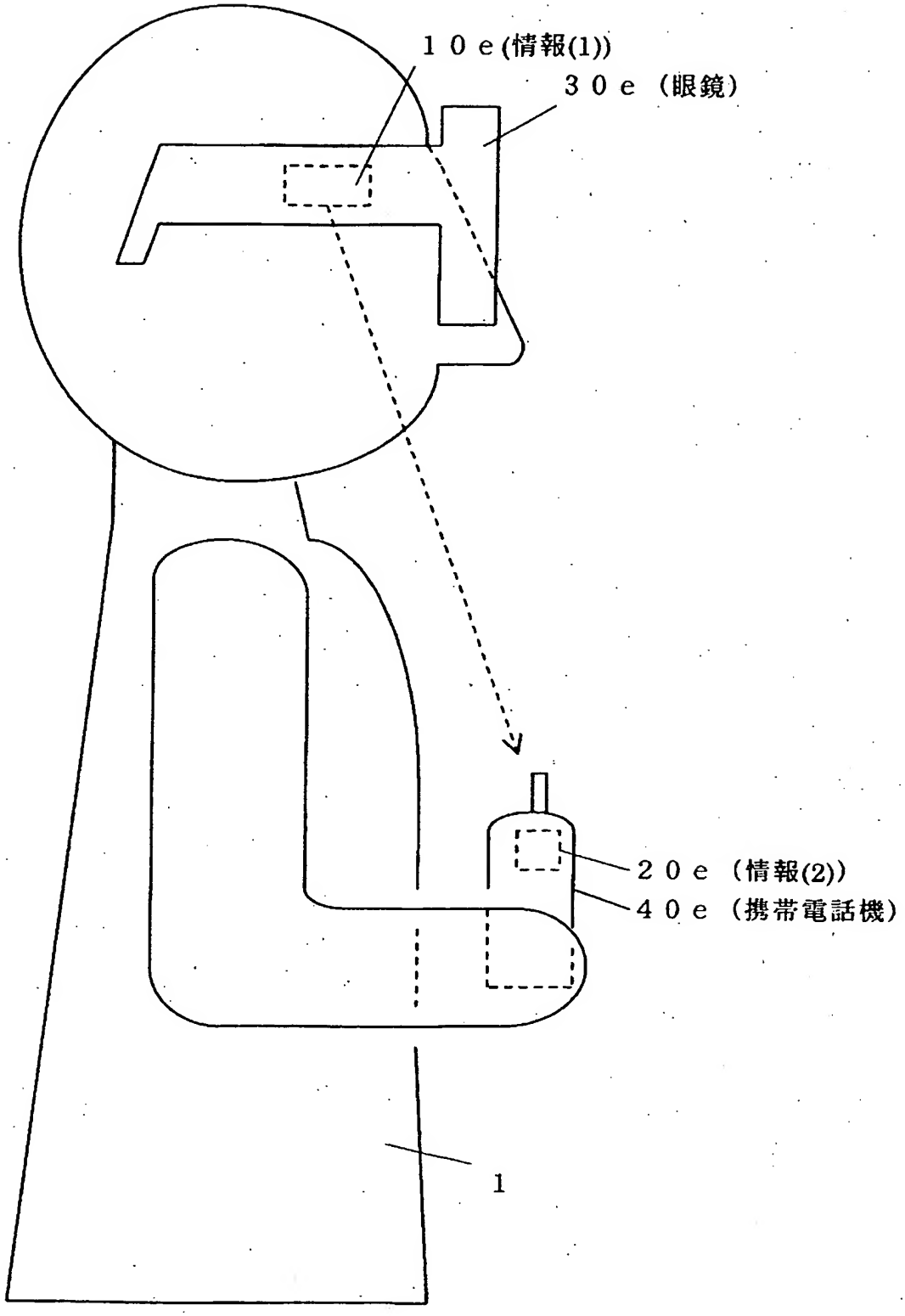


FIG. 10

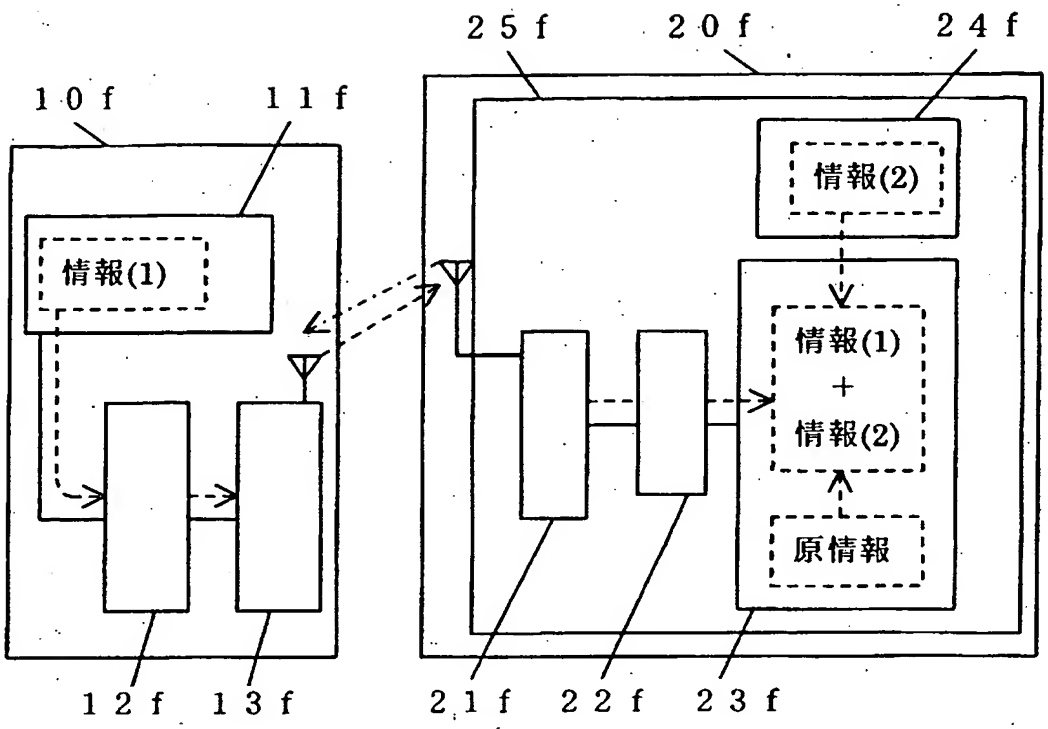

25f
20f
24f
10f
11f
情報(2)
情報(1)
情報(1)
+
情報(2)
原情報
12f
13f
21f
22f
23f

FIG. 11

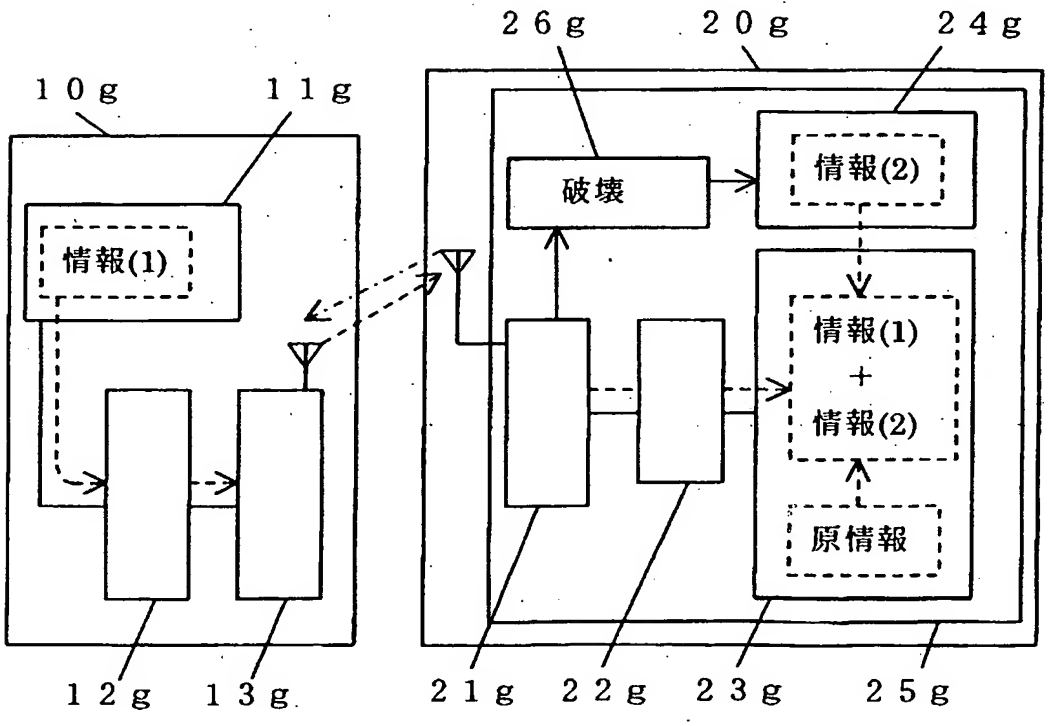

26g
20g
24g
10g
11g
破壊
情報(2)
情報(1)
情報(1)
+
情報(2)
原情報
12g
13g
21g
22g
23g
25g

FIG. 12

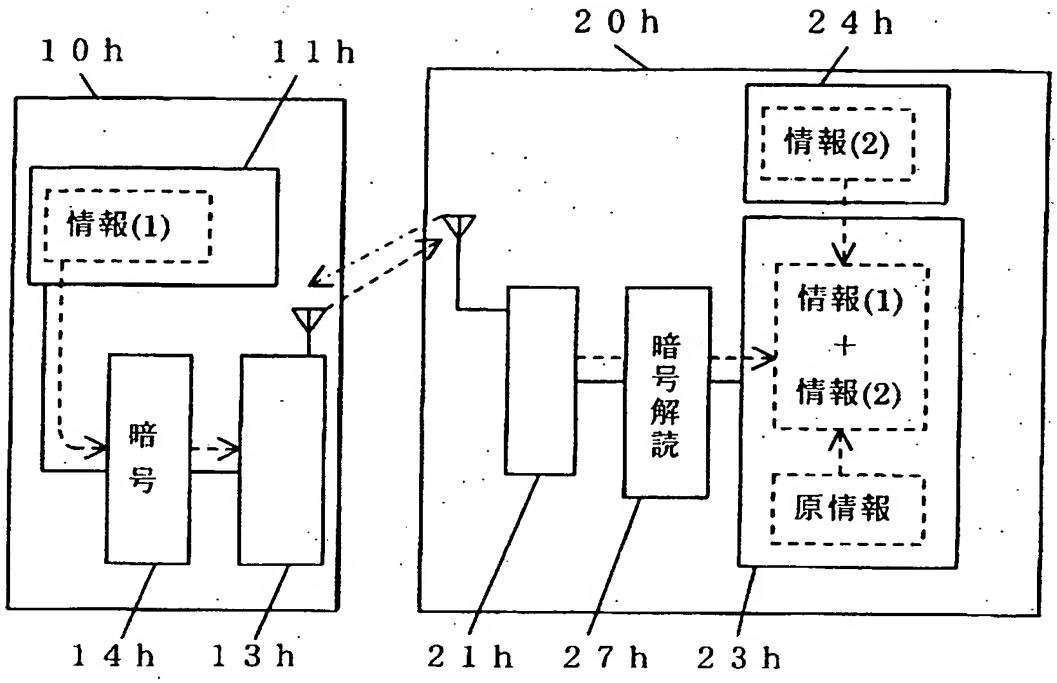

10h
11h
20h
24h
情報(1)
情報(2)
暗号
暗号解読
情報(1)
+
情報(2)
原情報
14h
13h
21h
27h
23h

FIG. 13

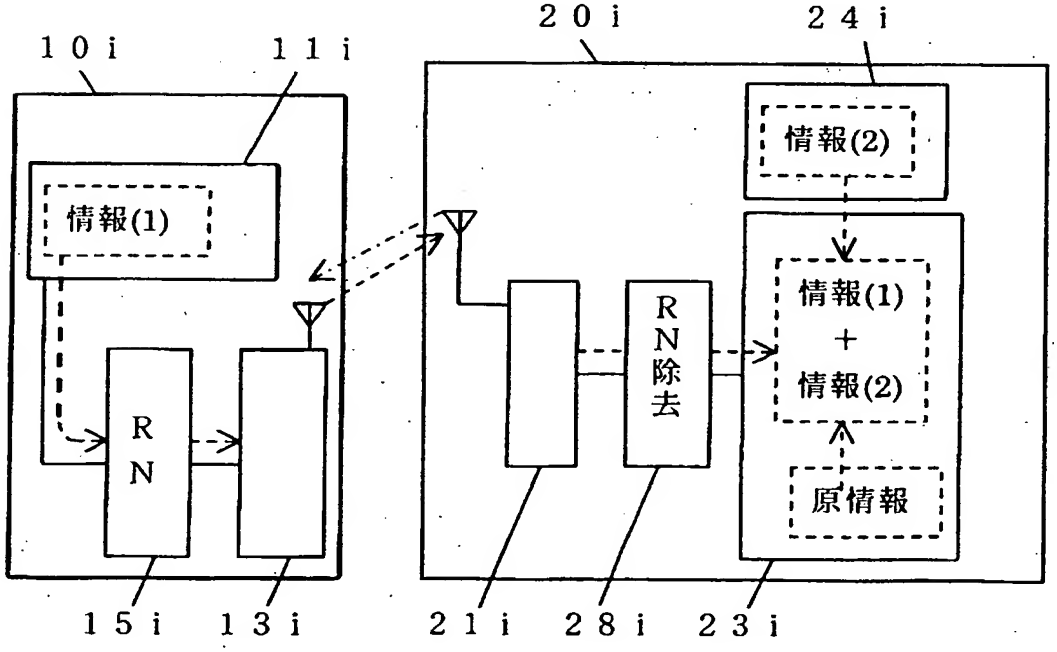

10i
11i
20i
24i
情報(1)
情報(2)
RN
RN除去
情報(1)
+
情報(2)
原情報
15i
13i
21i
28i
23i

FIG. 14

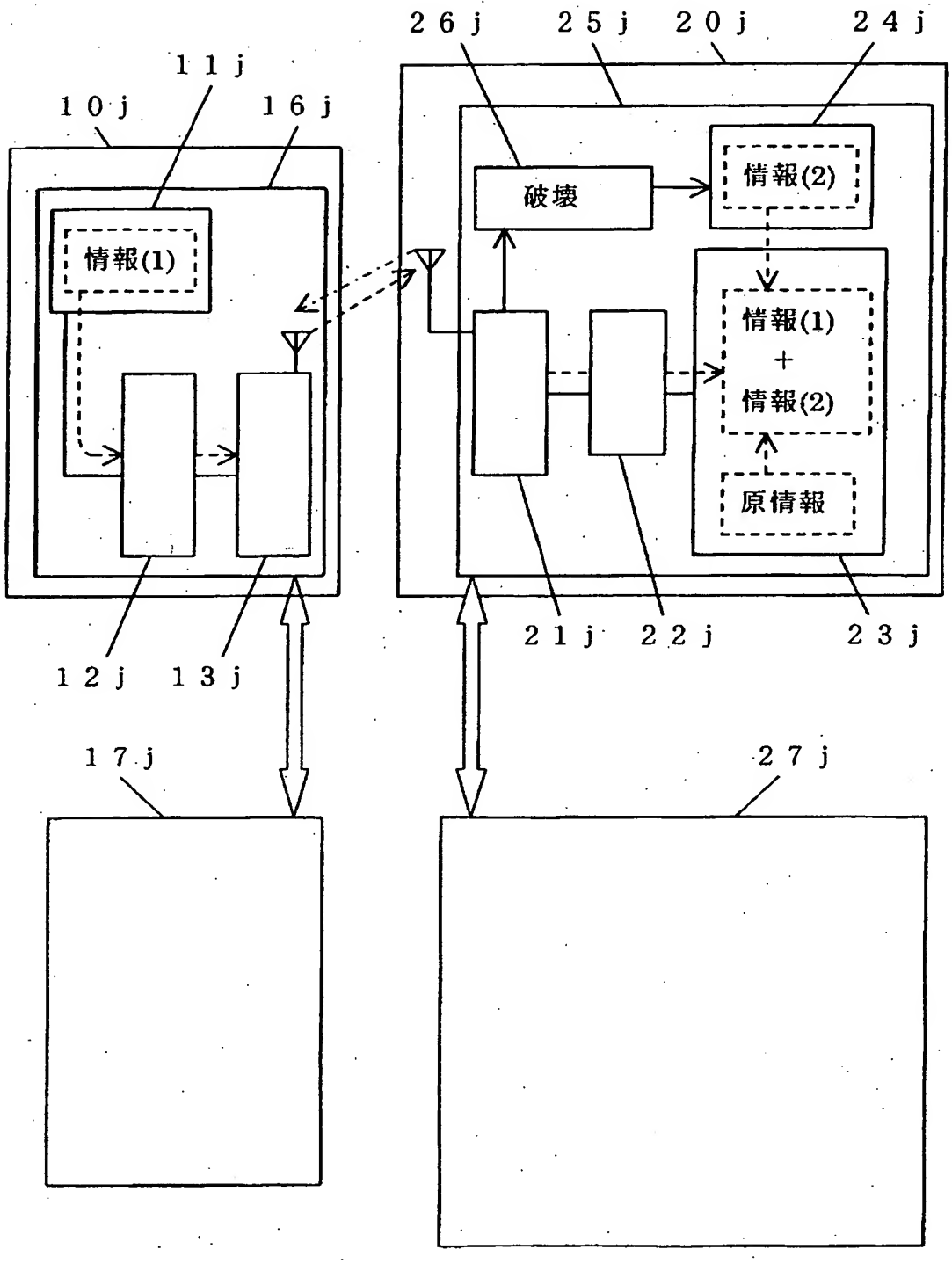

26j
25j
20j
24j
11j
10j
16j
破壊
情報(2)
情報(1)
情報(1)
+
情報(2)
原情報
12j
13j
21j
22j
23j
17j
27j

FIG. 15

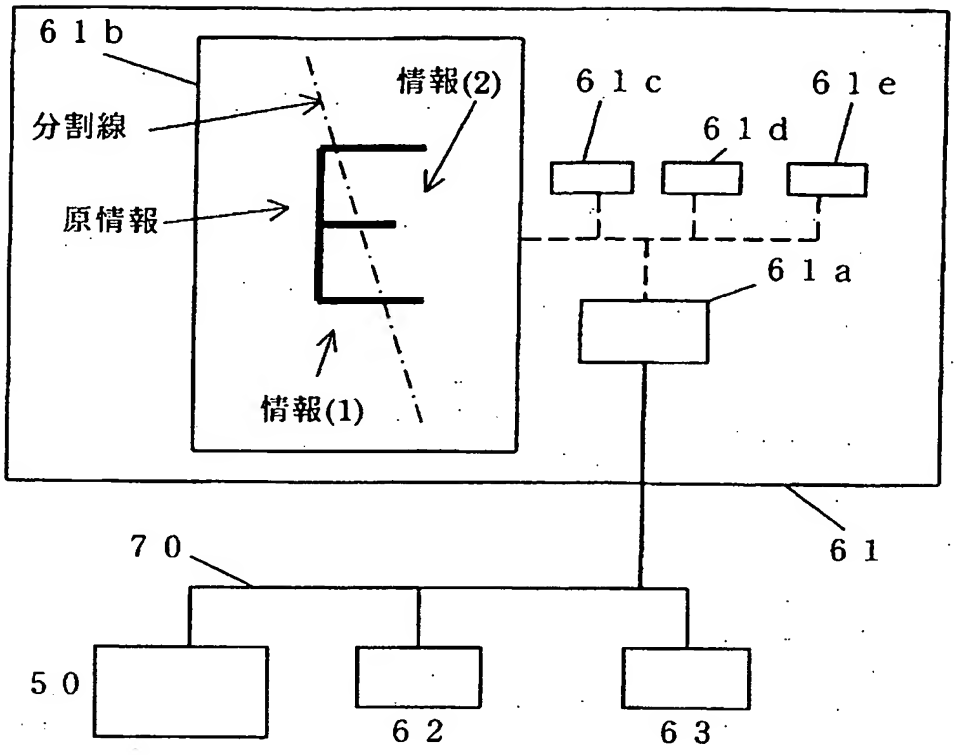

61b
分割線
情報(2)
原情報
情報(1)
61c
61d
61e
61a
61
70
50
62
63

FIG. 16

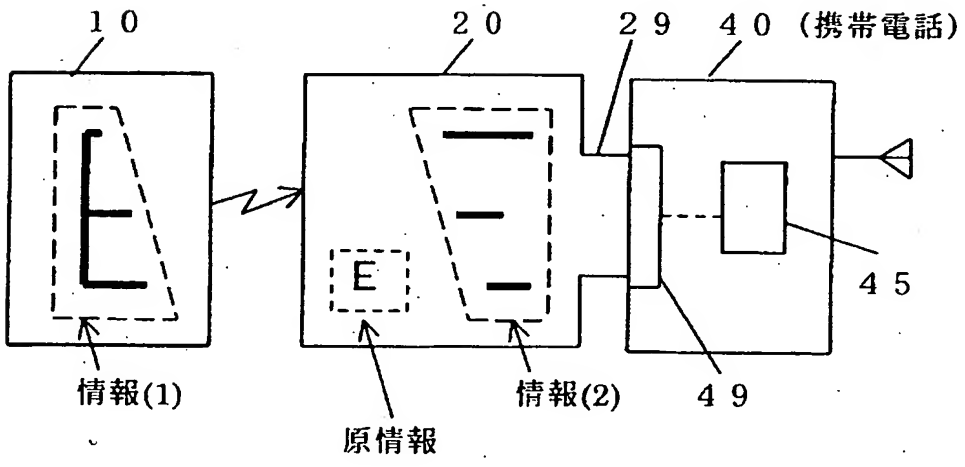

10
20
29
40 (携帯電話)
E
45
49
情報(1)
原情報
情報(2)

FIG. 17

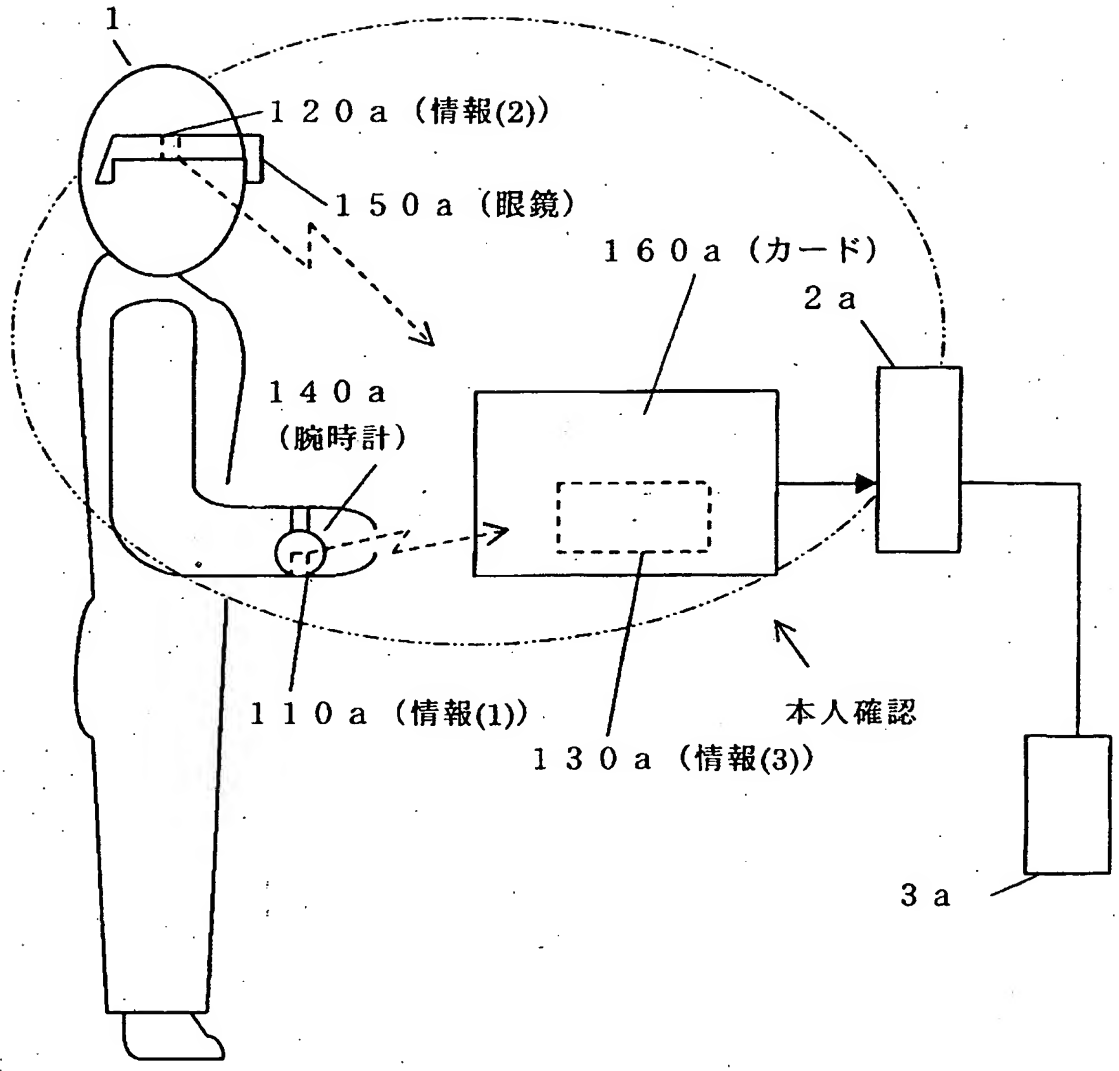

1
１２０ａ（情報(2)）
１５０ａ（眼鏡）
１６０ａ（カード）
２ａ
１４０ａ
（腕時計）
１１０ａ（情報(1)）
１３０ａ（情報(3)）
本人確認
３ａ

FIG. 18

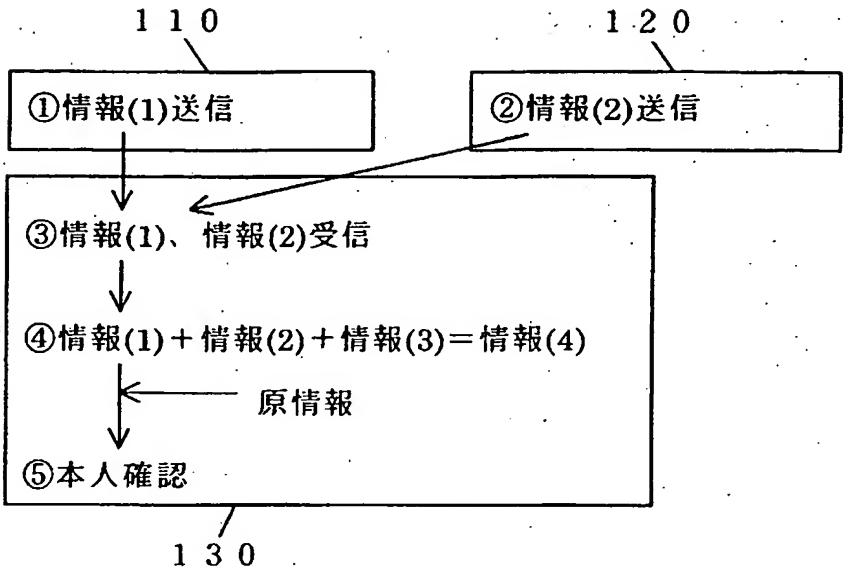

１１０
１２０
①情報(1)送信
②情報(2)送信
③情報(1)、情報(2)受信
④情報(1)＋情報(2)＋情報(3)＝情報(4)
原情報
⑤本人確認
１３０

FIG. 19

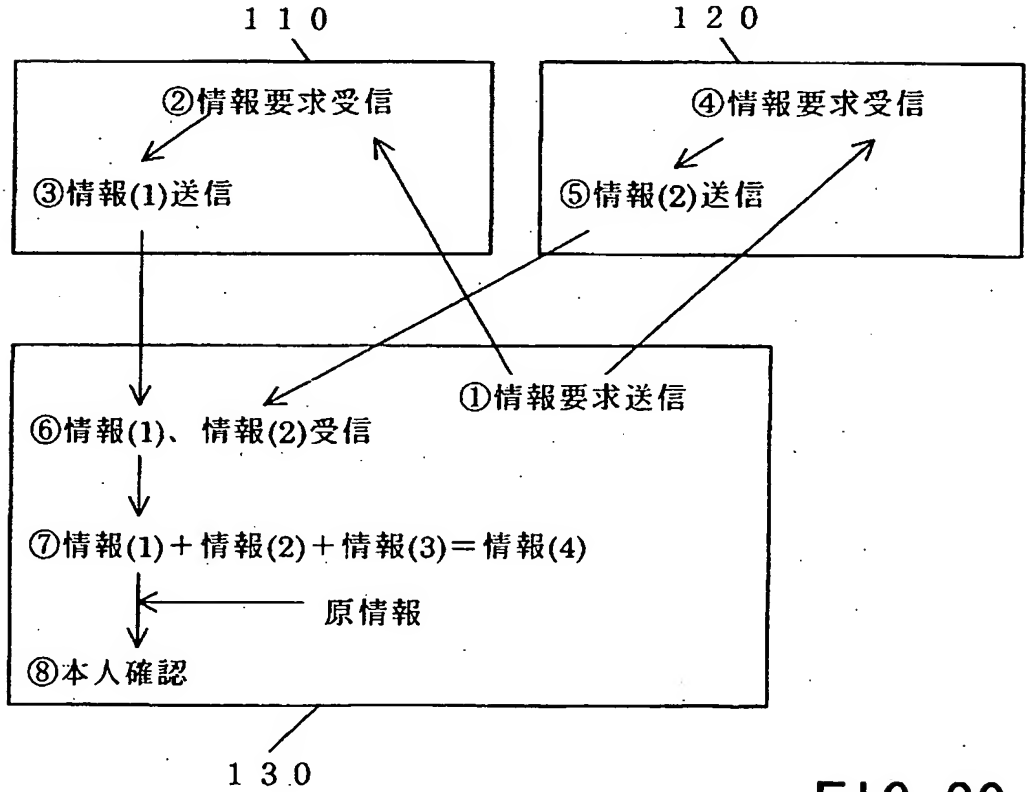

１１０
１２０
②情報要求受信
④情報要求受信
③情報(1)送信
⑤情報(2)送信
①情報要求送信
⑥情報(1)、情報(2)受信
⑦情報(1)＋情報(2)＋情報(3)＝情報(4)
原情報
⑧本人確認
１３０

FIG. 20

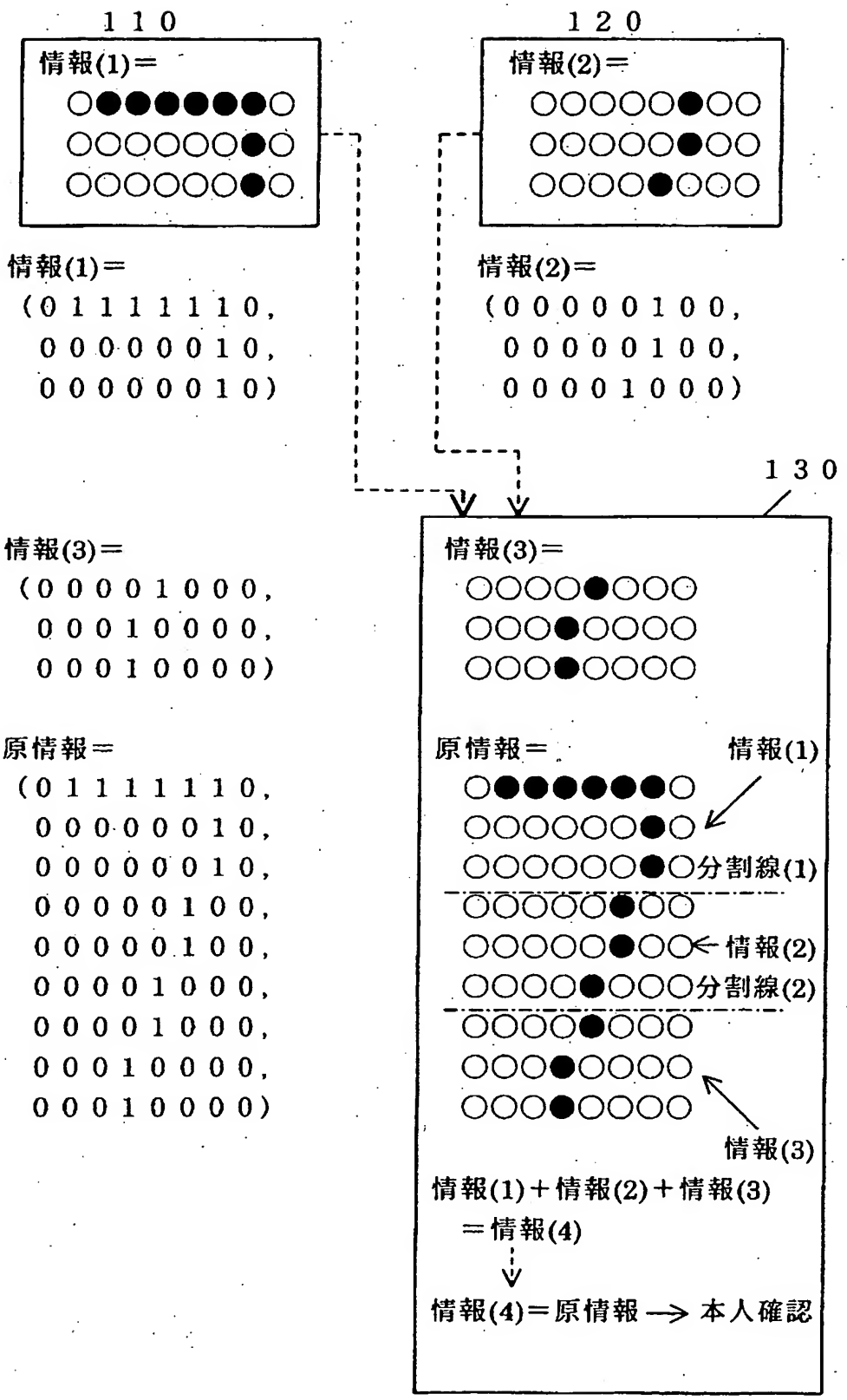

110
情報(1)＝
○●●●●●●○
○○○○○○●○
○○○○○○●○
120
情報(2)＝
○○○○○●○○
○○○○○●○○
○○○○●○○○
情報(1)＝
(0 1 1 1 1 1 1 0,
0 0 0 0 0 0 1 0,
0 0 0 0 0 0 1 0)
情報(2)＝
(0 0 0 0 0 1 0 0,
0 0 0 0 0 1 0 0,
0 0 0 0 1 0 0 0)
130
情報(3)＝
(0 0 0 0 1 0 0 0,
0 0 0 1 0 0 0 0,
0 0 0 1 0 0 0 0)
情報(3)＝
○○○○●○○○
○○○●○○○○
○○○●○○○○
原情報＝
(0 1 1 1 1 1 1 0,
0 0 0 0 0 0 1 0,
0 0 0 0 0 0 1 0,
0 0 0 0 0 1 0 0,
0 0 0 0 0 1 0 0,
0 0 0 0 1 0 0 0,
0 0 0 0 1 0 0 0,
0 0 0 1 0 0 0 0,
0 0 0 1 0 0 0 0)
原情報＝
情報(1)
○●●●●●●○
○○○○○○●○
○○○○○○●○分割線(1)
○○○○○●○○
○○○○○●○○ 情報(2)
○○○○●○○○分割線(2)
○○○○●○○○
○○○●○○○○
○○○●○○○○
情報(3)
情報(1)＋情報(2)＋情報(3)
＝情報(4)
情報(4)＝原情報 → 本人確認

FIG. 21

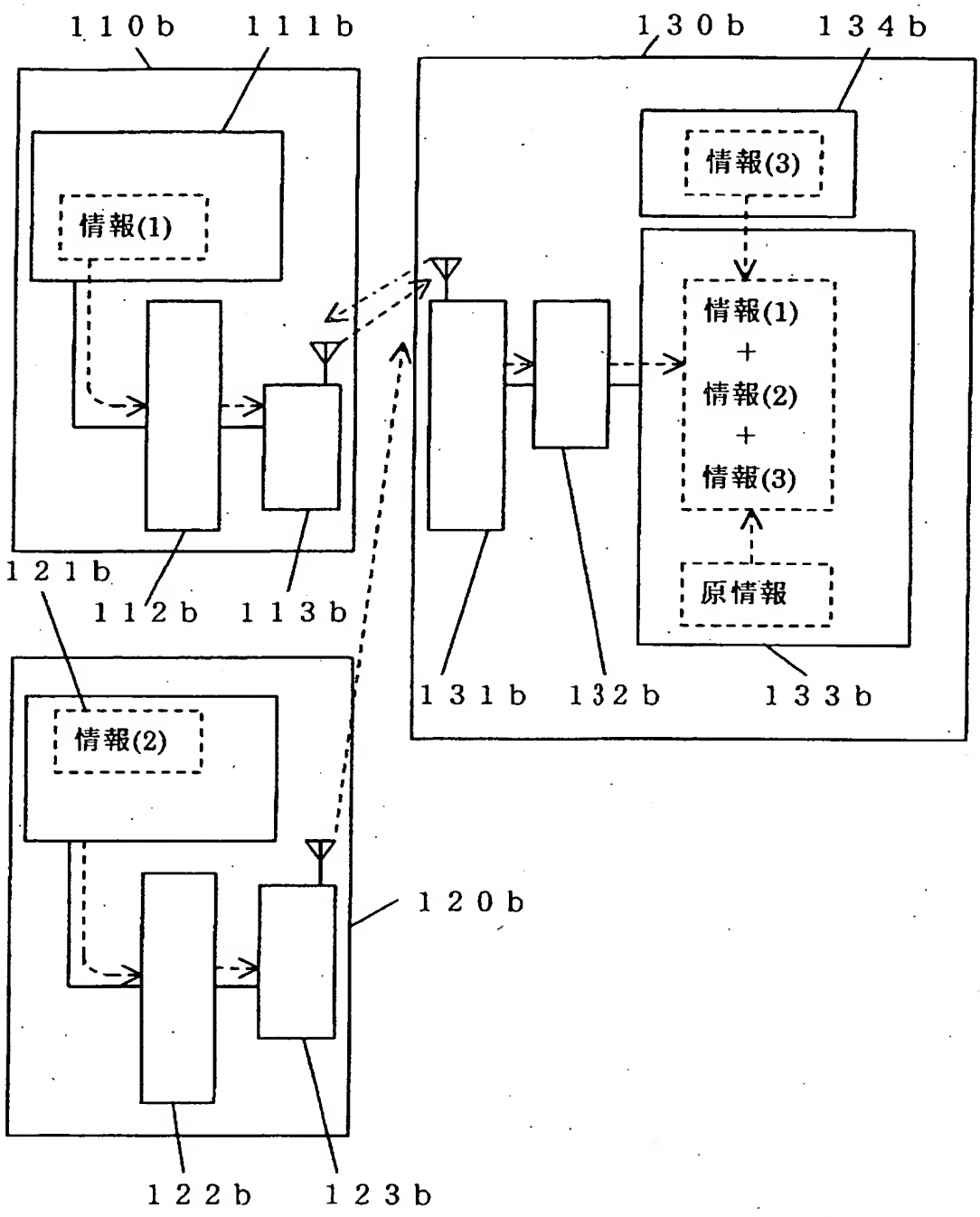

１１０ｂ
１１１ｂ
１３０ｂ
１３４ｂ
情報(1)
情報(3)
情報(1)
＋
情報(2)
＋
情報(3)
原情報
１２１ｂ
１１２ｂ
１１３ｂ
１３１ｂ
１３２ｂ
１３３ｂ
情報(2)
１２０ｂ
１２２ｂ
１２３ｂ

FIG. 22

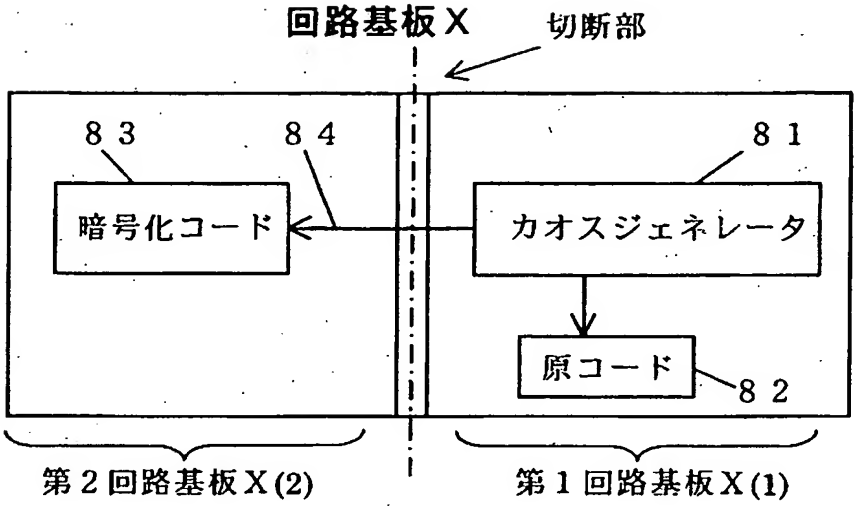

回路基板X
切断部
83
84
81
暗号化コード
カオスジェネレータ
原コード
82
第2回路基板X(2)
第1回路基板X(1)

FIG. 23

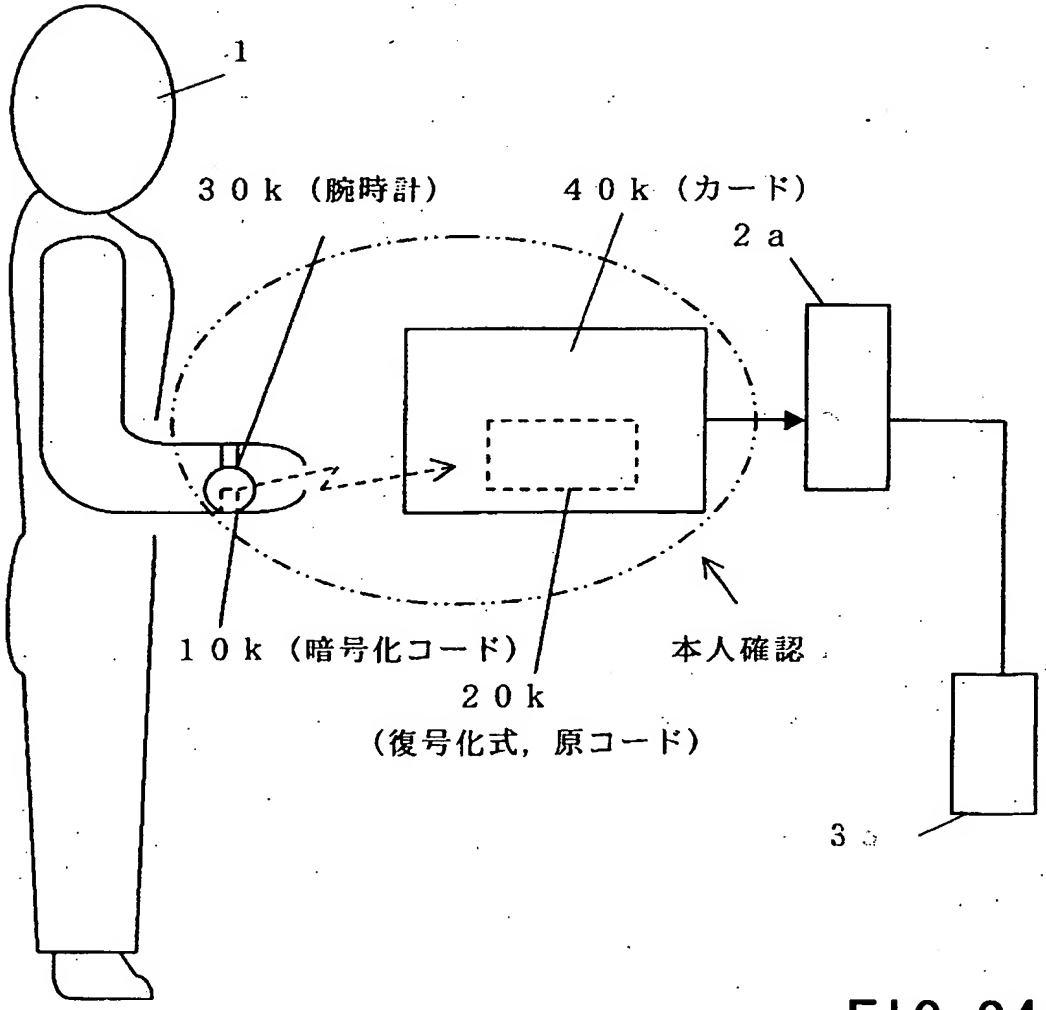

1
30k（腕時計）
40k（カード）
2a
10k（暗号化コード）
本人確認
20k
（復号化式，原コード）
3

FIG. 24

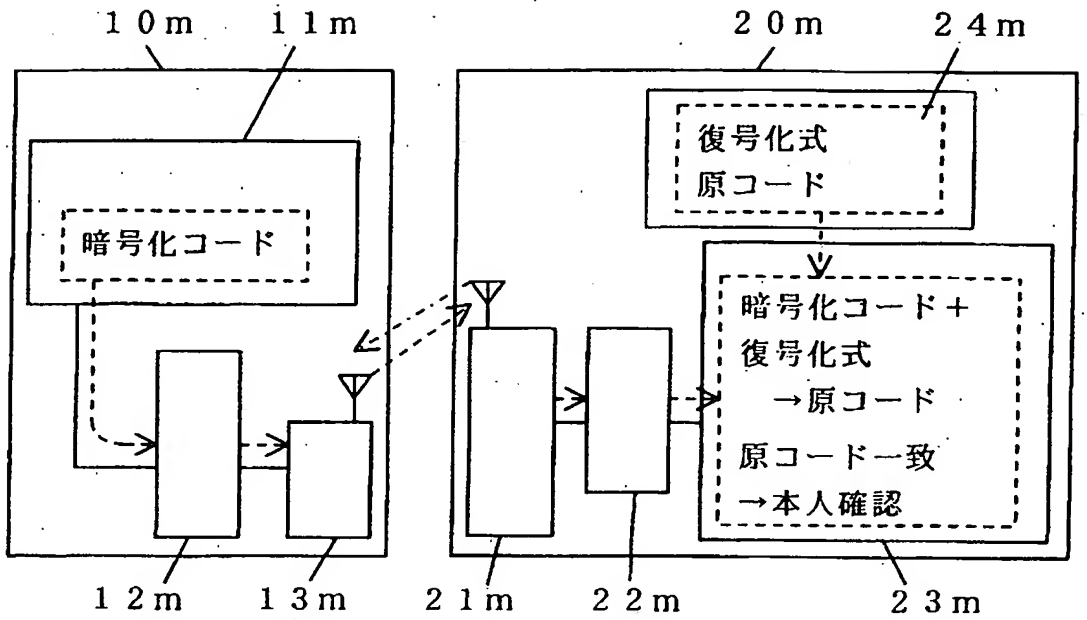

１０ｍ
１１ｍ
２０ｍ
２４ｍ
復号化式
原コード
暗号化コード
暗号化コード＋
復号化式
→原コード
原コード一致
→本人確認
１２ｍ
１３ｍ
２１ｍ
２２ｍ
２３ｍ

FIG. 25

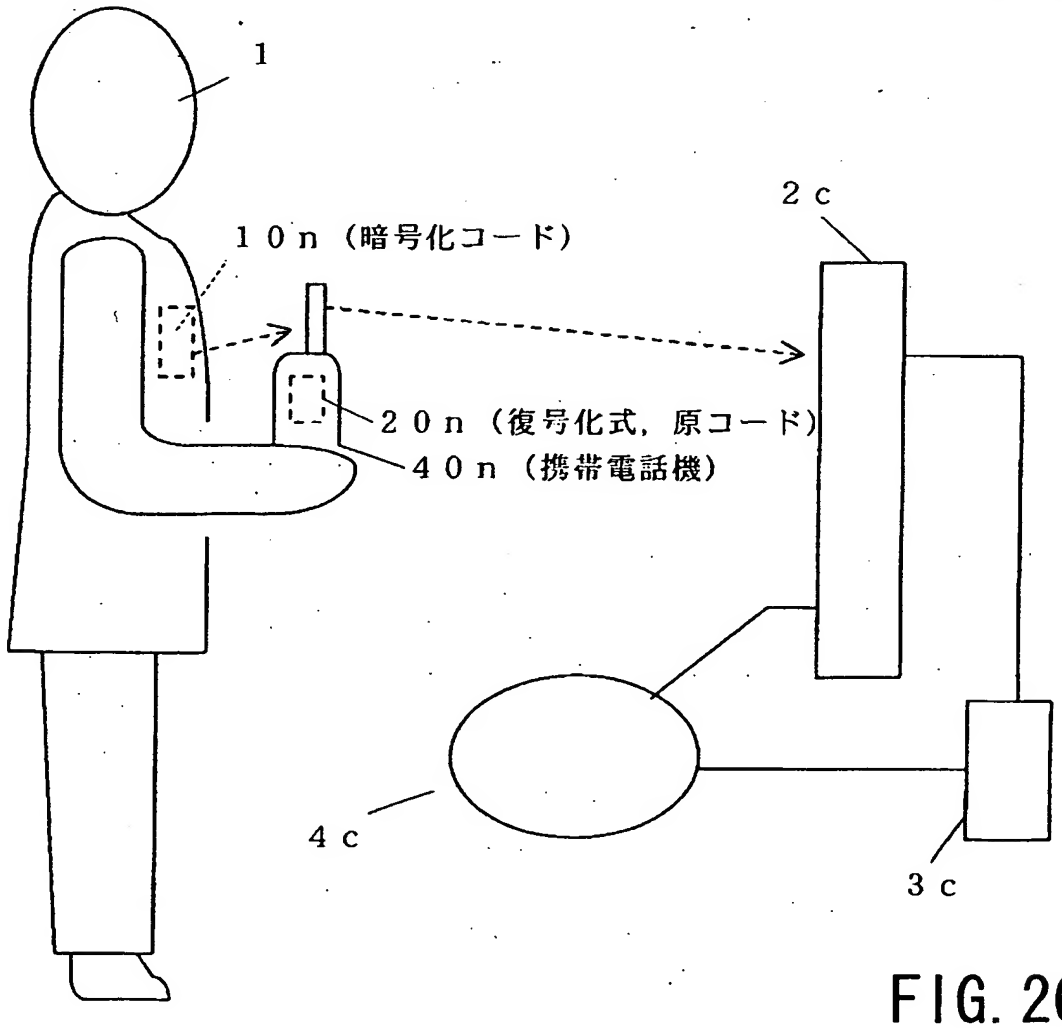

１
２ｃ
１０ｎ（暗号化コード）
２０ｎ（復号化式，原コード）
４０ｎ（携帯電話機）
４ｃ
３ｃ

FIG. 26

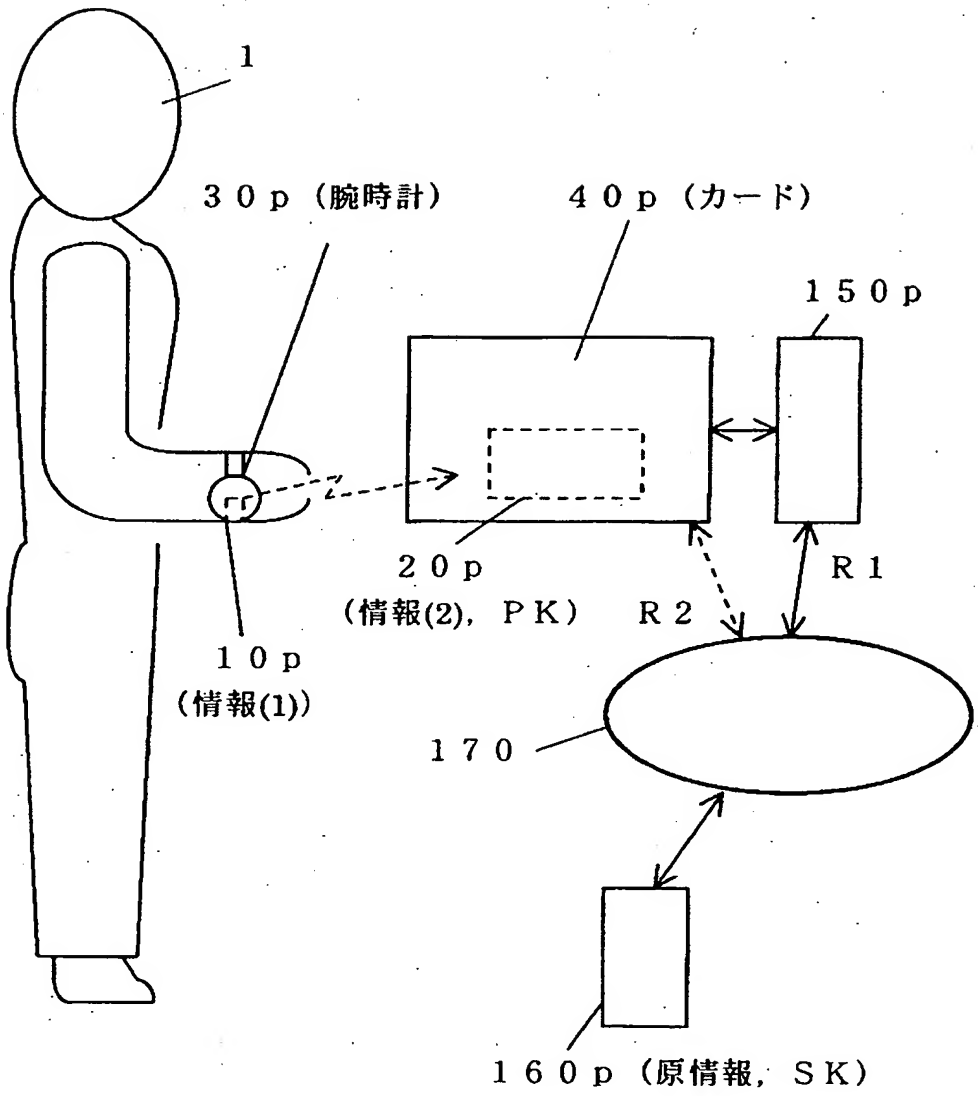


FIG. 27

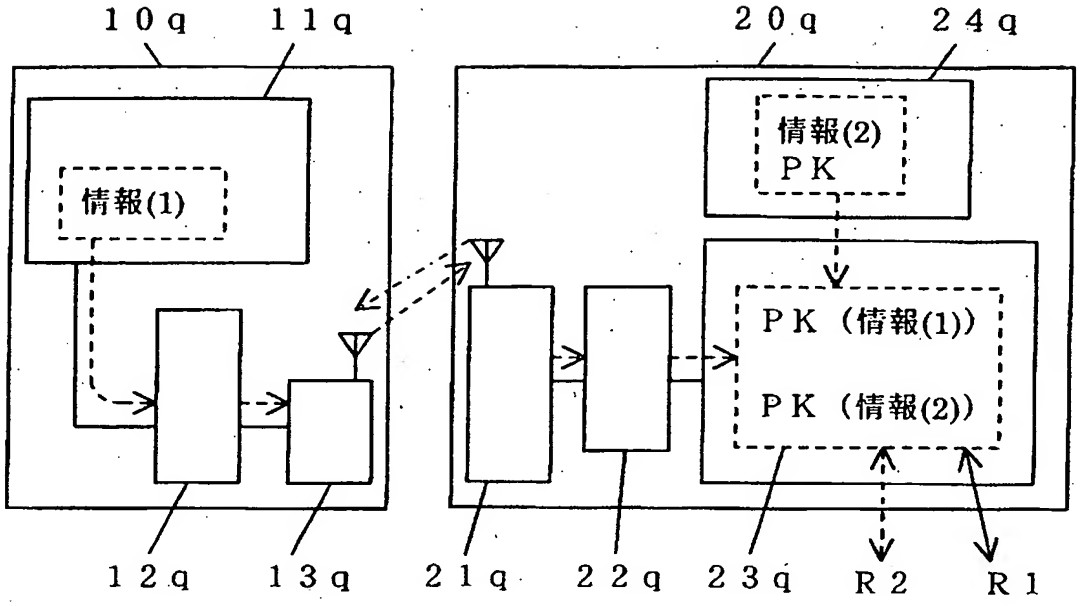

10q
11q
20q
24q
情報(1)
情報(2)
PK
PK（情報(1)）
PK（情報(2)）
12q
13q
21q
22q
23q
R2
R1

FIG. 28

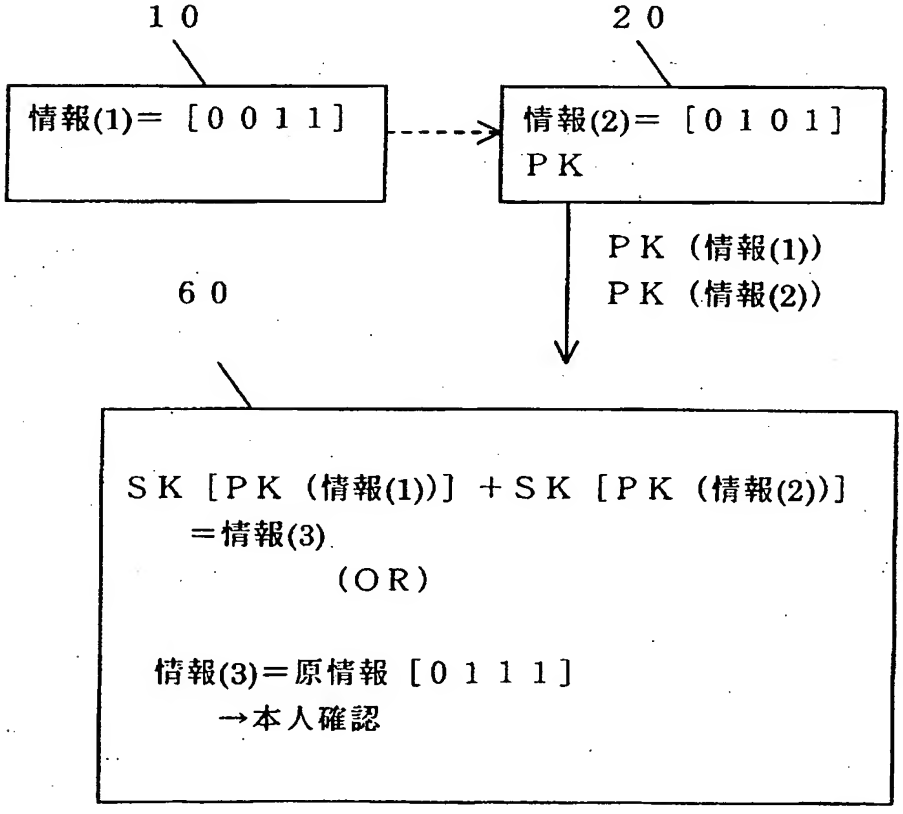

10
20
情報(1)＝［0011］
情報(2)＝［0101］
PK
PK（情報(1)）
PK（情報(2)）
60
SK［PK（情報(1)）］＋SK［PK（情報(2)）］
＝情報(3)
（OR）
情報(3)＝原情報［0111］
→本人確認

FIG. 29

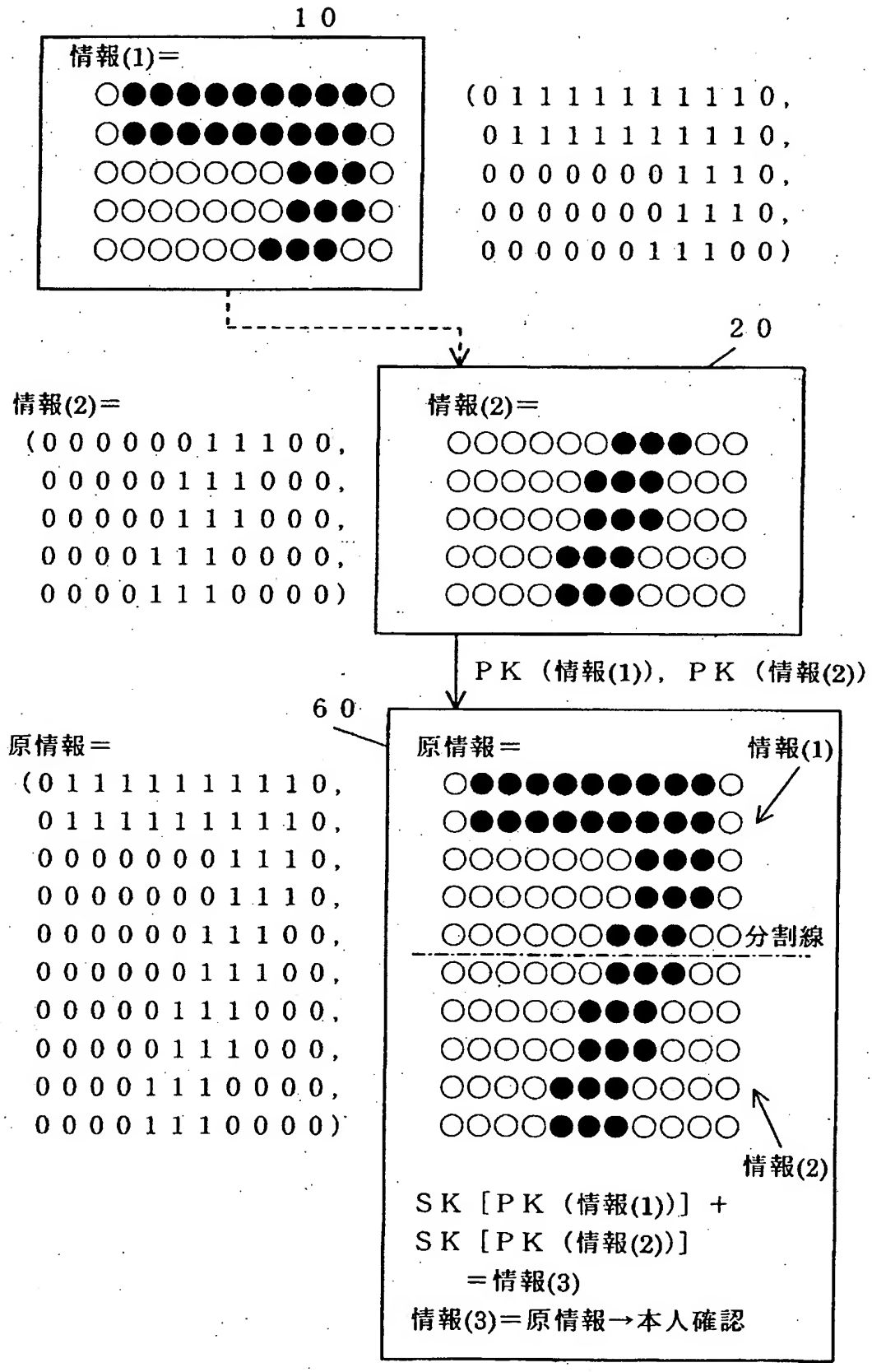

10
情報(1)=
(0 1 1 1 1 1 1 1 1 1 0,
0 1 1 1 1 1 1 1 1 1 0,
0 0 0 0 0 0 0 1 1 1 0,
0 0 0 0 0 0 0 1 1 1 0,
0 0 0 0 0 0 1 1 1 0 0,
0 0 0 0 0 1 1 1 0 0 0)
20
情報(2)=
(0 0 0 0 0 0 1 1 1 0 0,
0 0 0 0 0 1 1 1 0 0 0,
0 0 0 0 0 1 1 1 0 0 0,
0 0 0 0 1 1 1 0 0 0 0,
0 0 0 0 1 1 1 0 0 0 0)
情報(2)=
PK（情報(1)），PK（情報(2)）
60
原情報=
(0 1 1 1 1 1 1 1 1 1 0,
0 1 1 1 1 1 1 1 1 1 0,
0 0 0 0 0 0 0 1 1 1 0,
0 0 0 0 0 0 0 1 1 1 0,
0 0 0 0 0 0 1 1 1 0 0,
0 0 0 0 0 1 1 1 0 0 0,
0 0 0 0 0 1 1 1 0 0 0,
0 0 0 0 1 1 1 0 0 0 0,
0 0 0 0 1 1 1 0 0 0 0)
原情報=
情報(1)
分割線
情報(2)
SK［PK（情報(1)）］+
SK［PK（情報(2)）］
=情報(3)
情報(3)=原情報→本人確認

FIG. 30

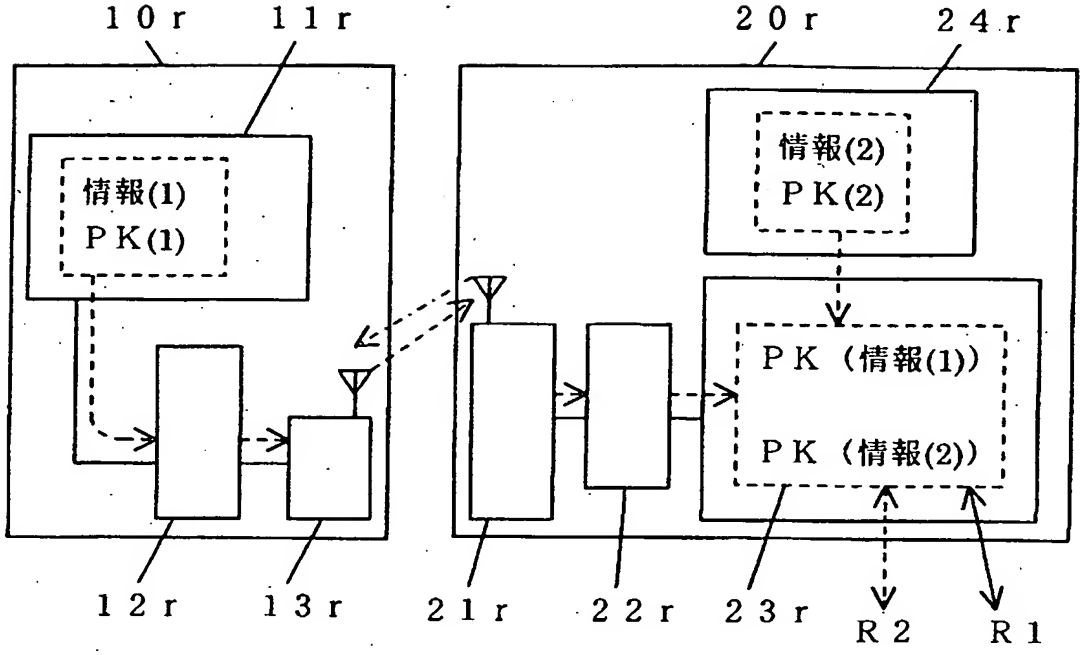

10r
11r
20r
24r
情報(1)
PK(1)
情報(2)
PK(2)
PK（情報(1)）
PK（情報(2)）
12r
13r
21r
22r
23r
R2
R1

FIG. 31

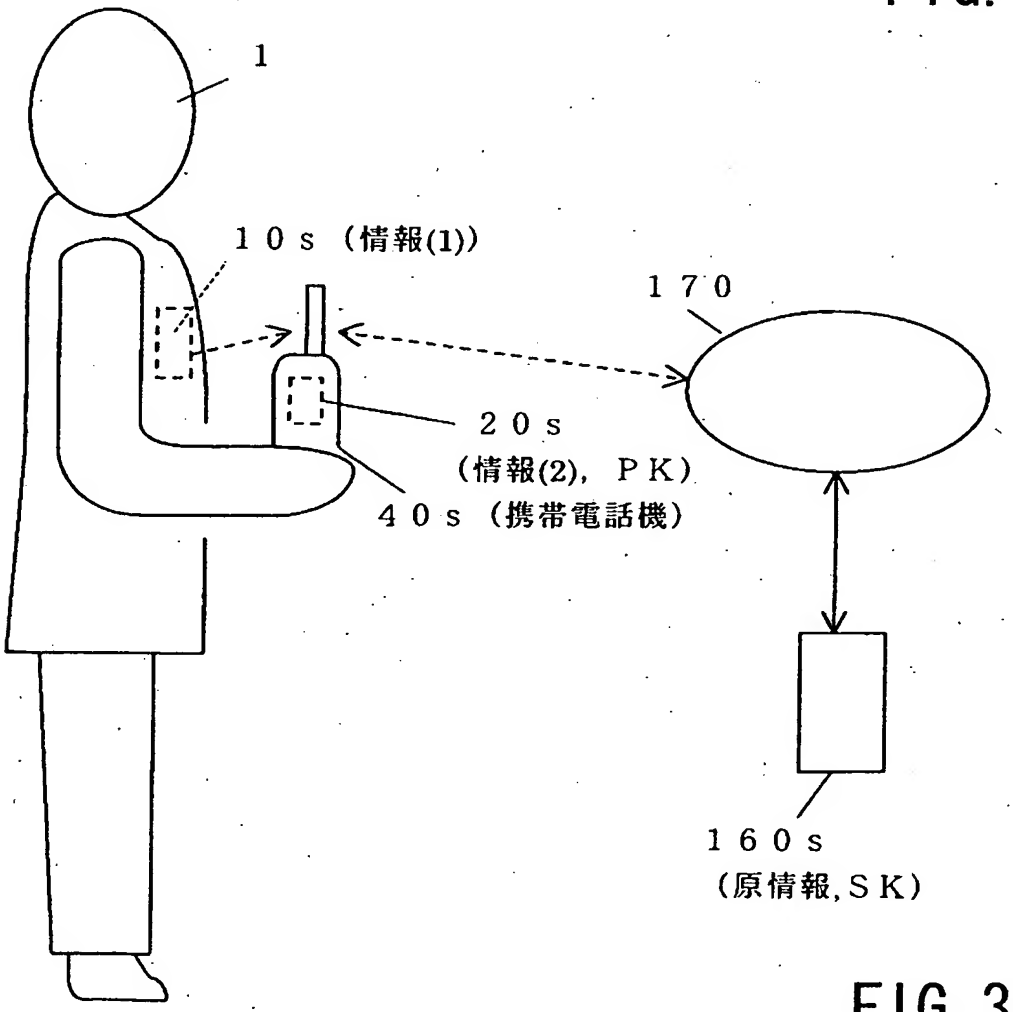

1
10s（情報(1)）
170
20s
（情報(2)，PK）
40s（携帯電話機）
160s
（原情報,SK）

FIG. 32

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/02329

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00, G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00, G06F17/60, G06K17/00, H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Toroku Jitsuyo Shinan Koho 1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP, 04-306760, A (Nippon Telegr. & Teleph. Corp. <NTT>), 29 October, 1992 (29.10.92) (Family: none) Full text	1-27 28-34
Y A	JP, 10-149339, A (Mitsubishi Electric Corporation), 02 June, 1998 (02.06.98) (Family: none) Claims	1-27 28-34
Y	JP, 11-167664, A (Nippon Conlux Co., Ltd.), 22 June, 1999 (22.06.99) (Family: none) Claim 6	3,10
Y	JP, 2000-11129, A (Nippon Telegr. & Teleph. Corp. <NTT>), 14 January, 2000 (14.01.00) (Family: none) description; Par. Nos. [0002] to [0004]	11,12
Y	JP, 10-322325, A (Shusuke YAMAJI), 04 December, 1998 (04.12.98) (Family: none) Claims	23,27

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 June, 2001 (13.06.01)	26 June, 2001 (26.06.01)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/02329

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 62-191198, A (Tokyo Tatsuno Co., Ltd.), 21 August, 1987 (21.08.87) (Family: none) Full text	31-34
A	JP, 04-335730, A (Toshiba Corporation), 24 November, 1992 (24.11.92) (Family: none) Claims	31-34

国際調査報告

国際出願番号 PCT／JP01／02329

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl' G06F15／00, G06F17／60

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl' G06F15／00, G06F17／60, G06K17／00, H04L9／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926－1996年
日本国公開実用新案公報 1971－2001年
日本国実用新案登録公報 1996－2001年
日本国登録実用新案公報 1994－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y A	JP, 04－306760, A（日本電信電話株式会社）, 29. 10月. 1992（29. 10. 92）（ファミリーなし） 全文	1－27 28－34
Y A	JP, 10－149339, A（三菱電機株式会社）, 2. 6月. 1998（02. 06. 98）（ファミリーなし） 特許請求の範囲	1－27 28－34
Y	JP, 11－167664, A（株式会社日本コンラックス）, 22. 6月. 1999年（22. 06. 99）（ファミリーなし） 請求項6	3, 10

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
13. 06. 01	26.06.01

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5B	9555
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	宮司 卓佳 電話番号 03－3581－1101 内線 3545		

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　PCT／JP01／02329

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP，2000－11129，A（日本電信電話株式会社），14．1月．2000（14．01．00）（ファミリーなし） 明細書第2段落～同第4段落	11，12
Y	JP，10－322325，A（山地秀典），4．12月．1998（04．12．98）（ファミリーなし） 特許請求の範囲	23，27
A	JP，62－191198，A（株式会社東京タツノ），21．8月．1987（21．08．87）（ファミリーなし） 全文	31－34
A	JP，04－335730，A（株式会社東芝），24．11月．1992（24．11．92）（ファミリーなし） 特許請求の範囲	31－34